Interest-driven Reasoning Based on Commitment Alternating Temporal Logic in the P2P Reputation System

Yu Bao
[a] Department of Computer Science and Technology, Tongji University, Shanghai, China
[b] Department of Computer Science and Technology, China University of Mining & Technology, XuZhou, China
Email: baoyucumt@126.com

Guo-sun Zeng
[a] Department of Computer Science and Technology, Tongji University, Shanghai, China
Email: gszeng@Tongji.edu.cn

Ke Zhang
Department of Computer Science and Technology, China University of Mining & Technology, XuZhou, China
Email: zhangke@cumt.edu.cn

***Abstract*—P2P files sharing system is popular in network applications. The trust evaluation, designed for restricting the malicious peers in the system, is often based on reputation. When peers choose the trust nodes to download files in terms of the trust evaluation, they have established trust among themselves. Besides the trust, the utility (or interest) gained by peers is the other important factor during the process. In order to find out how the system to evolve based on real utility and trust, we introduce a logic language of game theory, CATL, into the P2P reputation system of files sharing. We propose some deductive rules of strategy reasoning in terms of the utility of the peers to look for the trend of the node selection. The new logic tool works well and we analyze two cases based on it. One case, namely, "advertisement effect", blocks the newcomer and induces peers to collude with advocating reputation each other. The other case of "small-file-trend" constitutes a threat to the reputation system in Sybil Attack.**

***Index Terms*—P2P reputation system, strategy reasoning; trust, Commitment alternating temporal logic, CATL**

I. INTRODUCTION

During the process of information exchanging, the network entities are faced with the problem of how to establish trust among themselves. Web services depend on their Qos data described by WSDL, SOAP, and UDDI. Therefore, the user can decide which is better by computing the claimed data and the feedback data from the service or other users [1, 2]. However, the users in P2P are in different situation because it is difficult to locate the nodes. If the P2P file sharing system can be taken as a repeated game [3], many P2P systems use the KWRM principle [3] to establish trust system by rating the download files. When a user wants to download a file from one node, he would collect the node's historical transaction records and compute the trust value [1, 4, 5, 6, 7, 8].

P2P trust system depends on reputation gained in the repeated game. We use the trust to make decisions. Li [1] discusses the services selection of web services that rely on the feedback data. Despotovic [9] shows a probabilistic technique of maximum likelihood to estimate the percentage of liars in P2P system. Then the peers can establish trust by evaluating whether the opponent is a liar. Li and Despotovic propose a way to establish trust for choosing trust peers but do not discuss influencing factors. The Trust managements, such as EignTrust [4] and Peertrust [5], take into consideration of the trend of the system evolution to restrict the malicious behavior. Most of them try to do so through the protocols with trust value. However, the trust value is a computation about the history of observed behavior, transaction record, etc. Peers compute the value and select the antagonist according to the value. Therefore, many researches focus on the computation methods such as the algorithms in Ref. [4, 5, 6, 10]. Researchers have worked out some efficient methods. Jøsang [7, 11, 12] introduced *subjective logic*, a trivalent logic, into the trust system called TNA-SL. He tried to denote the uncertain value, besides truth and false value, dividing the observed behavior with belief. He optimized the network by deriving trust from parallel paths. Zhang [8] and Sherchan [13] proposed a new method with Fuzzy logic. Their works are similar to Jøsang's in the way to deal with the trust value reasoning, but they focused on the reputation or trust computation and separate it from the real utility between the entities.

doi:10.4304/jcp.5.12.1942-1950

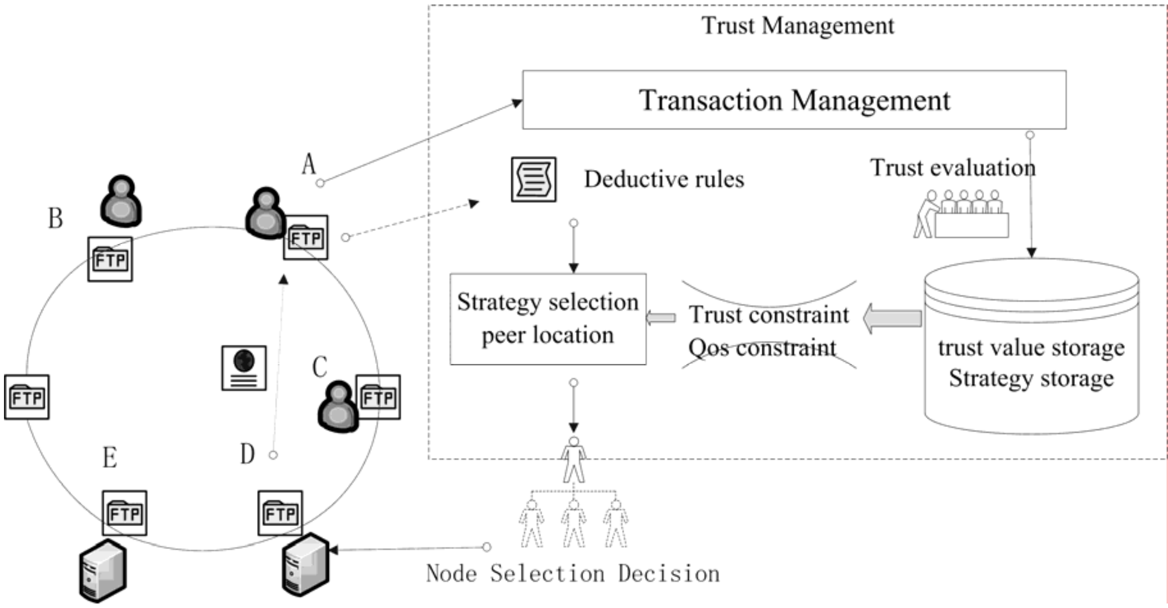

Fig.1 TTP Trust Management Structure in P2P file sharing system (Trust storage saves the value of evaluated value according to transaction. Peers selection follows these values by choosing strategy on its' own shoes.)

We believe that the rational peers in the system would be in theirs' own shoes because of self-interests. From the viewpoint of game theory, each peer would select the best strategy in different contexts for the sake of the maximization utility. Some former researches [14] paid more attention to build the model or protocol according to game theory. Harish [15] focused on the static game and proposed a trust management including some game strategies like tit-tat strategy. Komathy [16] designed a game strategy for the routing in Ad Hoc net. His rules constrain selfishness in forwarding process and include incentives for cooperation. Mobasherl [17] proposed the profiles injection attacks and illustrated why the hybrid attack had advantages in terms of attack cost. These researches show that the utility of the peers is an important factor in trust establishing process.

However, we find nodes in P2P system are interest in sharing files because they can gain utility. In terms of this, we divide the trust computation into two parts. One is the reputation and the other is the interest. Another consideration is temporal property that the system changes with time.

For analyzing the trust-driven changes triggered by utility and the temporal property, we need tools for reasoning based on game theory. Jamroga [18] tried to do it and extended the language of ATL [19] with operators of plausibility to reason about the behavior and abilities of agents. However, he did not take into account the utilities of entities and his theory lack the special deductive rules to decide what the peers want to choose. We will introduce a logic language, CATL [20, 21, 22], which is proper for multi-player and strategy reasoning, to describe the model of the P2P files sharing system.

In files sharing system, the peers establish trust when the they select the cooperative node according to the context, and the constraints. The peers' selection is another aspect of establishing trust. We analyze the peers' selection and investigate what may influence the selection process of trust node, and how to win the game and gain more in the system, and what is the trend is for the system running. That is the motivation of this paper.

One of our contributions is to describe the selection game by introducing CATL (Commitment alternating temporal logic) into P2P reputation system. Secondly, we come up with some new deductive rules of the CATL according to the actual and trust utility. Then armed with the tool, we find out the "advertisement effect" and "small-file-trend" in P2P file-sharing system. Then we interpret these phenomenon effects in the files sharing system by CATL.

The rest of this paper is organized as follows. Section 2 introduces the model of P2P file-sharing system based on CATL and AATS (action-based Alternating Transition System). Section 3 describes the constraints and deductive rules in the model. We use the rules to describe the "advertisement effect" and "small-file-trend" in section 4 and 5 respectively. Finally we come to a conclusion in section 6.

II. P2P File - Sharing Model and its Description

A. P2P Files Sharing System Based on Reputation

The work of P2P file sharing system is illustrated in figure 1. When peer *A* searches a file, it is going to send request to its neighbors *B* and *C*. If *B* or *C* has the file, they would offer it; if not, they would forward the request to their neighbors. Node *A* eventually receives a set of nodes that may have the file. Then *A* will decide which one or subset may be the best trustees by evaluating their historical transactions record obtained from their neighbors. According to the decision, *A* downloads the file from these trusted nodes.

In that process, two problems should be solved. The first problem is how to limit the free-riding behavior. A game of file flow of each node is adopted so that the nodes with more contribution can download more. The second is how to evaluate the transactions. In general, evaluation is done by labeling the quality of the download file with a number as soon as downloading finishes. The number is, often "1" (denotes good quality) or "0" (denotes bad quality), called reputation value. When one peer wants to select a trustee, it will try its best to collect all the reputation data from other peers that have the transaction record with the candidate. Then it computes a trust value of the candidate by formula and the result is a real value in [0, 1]. Furthermore, the system introduces a threshold. If the trust value is more than threshold, the trustee peer is chosen.

Suppose the peer selection of P2P file sharing system is a game, each peer is the participant who chooses his strategy of downloading and uploading to make profit maximized. We call the trustee nodes "antagonist" or "opponent" in the game. A game model is M= (GAG, {GAC},{Gu}), where GAG =<a_1, ..., a_n>, { GAC } is the actions set, {Gu} is the utility function that assigns the real-valued utility to each combination of players' strategy.

In this model, we need to analyze the game between the nodes, including the nodes' strategy, the deductive rules, and the time over which P2P file sharing changes. This needs a temporal transition system that can describe P2P sharing system as time varying. AATS, a transition system based on action, has the temporal property to do so. We use the CATL to descript the P2P reputation system states for mapping them to AATS.

B. Grammar and Semantic of CATL for Multi-player Game

CATL is generation of ATL [19] that maps the game actions to the state of transition system based on AATS. AATS adds the action set and strategy set to the traditional ATS to analyze the player's behavior. When one selects a strategy, he would follow the strategy to transmit his state. Therefore, the CATL can map the game process of player's selection to the AATS. The AATS is denoted as follows:

Definition 1 (**AATS**)[20, 22] denotes as a tuple $M=(Q, Q_0, P, \pi, Ag, Ac, \rho, \tau, \Upsilon, \Sigma, \|\bullet\|)$

Where:

Q: a non-empty set of states of the system and we assume the system is in one of state.

Q_0: the initial states;

P: a finite, non-empty set of atomic propositions.

π: $Q \rightarrow 2^P$ is an interpretation function.

Ag: an agent set, finite and non-empty, which members are the game players.

Ac: the action set of the agents.

ρ: $Ac \rightarrow 2^P$ is the action precondition function that defines in which state the action in Ac may be executed.

τ: $Q \times Ac \rightarrow Q$ is a partial system transition function that defines how to determine the next state for a particular state q and a tuple of valid decisions from all the agents in q. It is consistent with function ρ.

Υ: The *strategy term* set. AATS uses the *strategy terms* to address each single-step action occurred in states.

Σ: Strategy set, we denote strategies of agent a_i as Σ_i. A strategy for an agent is a function: σ_i: $Q \rightarrow Ac$ which must satisfy the constraint that the action is available for the agent in state $q \in Q$.

$\|\bullet\|$: $\Upsilon \rightarrow \Sigma$, gives a denotation of every strategy term.

If we define a computation as an infinite sequence of states $\lambda = q_0, q_1, \ldots$, a *computation* starting in state q is named as *q-computation* . If $v \in \aleph$, and $\lambda[v]$ is used to denote the state located at the place v in λ; ($\lambda[0]$ denotes the first element, $\lambda[1]$ the second, and so on). Moreover, given a state q and strategy σ_i of agent i, $comp(\sigma_i, q)$ means the possible computation starting at the state q when agent i selects the strategy. For a given state q and σ_i, $comp(\sigma_i, q)$ is singleton. CATL contains some temporal operators. The □ temporal operator means "now and forever more", ○ "next" and U "until". The additional temporal operator ◊ can be replaced by $\Diamond\varphi = \top \, \mathcal{U} \, \varphi$($\top$ is true). Besides these temporal operators, CATL adopts the "committing to" operator "C" to indicate strategy selection. The ternary modal $C_i(\sigma_i, \varphi)$ means "suppose agent i chooses the strategy σ_i then the proposition φ holds". After choosing the special strategy q, we obtain the AATS relative to the strategy by the commitment operation †. For instance, $q\dagger\sigma_i$ is "AATS obtained by eliminating all the states that are not consistent with the strategy σ_i" [20]. The syntax of CATL is given by the following grammar [20]:

$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \psi \mid C_i(\sigma_i, \varphi) \mid \langle\langle A\rangle\rangle \circ \varphi \mid \langle\langle A\rangle\rangle \Box \varphi \mid \langle\langle A\rangle\rangle \varphi \, \mathcal{U} \, \psi$

Where: $p \in \Phi$ is the proposition variable, $i \in Ag$, $A \subseteq Ag$ is an agent set and $\sigma_i \in \Sigma_i$ is one strategy of agent i(not included in φ).

The semantic of CATL [20] is illustrated by AATS and the definition of the formula is given below:

(1) $q \models p$, iff $p \in P$, and $p \in \pi(q)$;

(2) $q \models \neg\varphi$, iff $q \not\models \varphi$;

(3) $q \models \varphi \vee \psi$, iff $q \models \varphi$ or $q \models \psi$;

(4) $C_i(\sigma_i, \varphi)$, iff $q\dagger\sigma_i \models \varphi$;

(5) $q \models \langle\langle A\rangle\rangle \circ \varphi$, iff $\exists \sigma_A \in_A$,such that $\forall \lambda \in comp(\sigma_A, q)$,we have $\lambda[1] \models \varphi$

(6) $q \models \langle\langle A\rangle\rangle \Box \varphi$, iff $\exists \sigma_A \in \Sigma_A$,such that $\forall \lambda \in comp(\sigma_A, q)$ and $v \in \aleph$, we have $\lambda[v] \models \varphi$

(7) $q \models \langle\langle A\rangle\rangle \varphi \, \mathcal{U} \, \psi$ iff $\exists \sigma_A \in \Sigma_A$, such that $\forall \lambda \in comp(\sigma_A, q)$ and $v \in \aleph$, we have $\lambda[v] \models \varphi$, and for all $0 \leq v' \leq v$, we have $\lambda[v'] \models \psi$。

The other connectives ("∧", "→", "↔") can be defined by "¬" and "∨". The modal operator U can be used instead of "◊", for example, $\langle\langle A\rangle\rangle \Diamond \varphi$ is an abbreviation of $\neg\langle\langle A\rangle\rangle \top \, \mathcal{U} \, \varphi$. We write $\langle\langle 1, 2, \ldots \rangle\rangle$ rather than $\langle\langle \{1, 2, \ldots\} \rangle\rangle$.

C. P2P Files Sharing System Model Based on CATL

If we want to map the P2P files sharing system to AATS, we would translate the observed behaviors into atomic propositions. The action set of a node a_i is {GAC}={uploading file, downloading file, searching information of file, searching a node history record, rejecting a requisition, computing a node trust value, recommending a node, making a selection, doing nothing}. For simplicity, we omit some actions, such as answering a request, forwarding requests, etc., because they do not affect peers interests. We use GD_i to denote the nodes set that have downloaded files from a_i, GU_i to denote the nodes set from which a_i has downloaded files.

The behaviors of peers are the strategy selection. Therefore, Υ maps to {*GAC*} and we get a_i strategy term set shown as predication. Υ= { $ULF(f, a_i)$ (denotes a_i upload file f), $ULQ(Q^{ul}_i, a_i)$ (denotes a_i uploading the file of quality Q^{ul}_i)), $ULS(SP^{ul}_i, a_i)$ (a_i uploading the file with speed SP^{ul}_i), $DLF(f, a_i)$ (denotes a_i download file f), $DLQ(Q^{dl}_i, a_i)$ (a_i downloading file of quality Q^{dl}_i), $DLS(SP^{dl}_i, a_i)$ (a_i downloading the file with speed SP^{dl}_i), $SCH(a_i)$ (sending searching message to a_i), $REQ_i(a_j)$ (a_i requests the file from a_j), $DNY(a_i)$ (rejecting the peer a_i download requisition), $RC_i(a_j, a_k)$ (the peer a_i receives recommendation of a_k from a_j), $COL_i(a_j)$ (a_i collecting the reputation value of a_j), $CP_i(h_{i,j}, h_{k,j}$ where $a_k \in GD_j \setminus a_i$) ($a_i$ computes the trust value TR_j of a_j), $Ac_i\varphi$(denotes a_i do nothing}. Where SP^{ul}_i and SP^{dl}_i satisfy strictly continuous and increasing in the real interval [0,X]. The additional predications will be discussed below. The subscript of predications denotes the owner. For example, j in $REQ_j(a_i)$ is the requisition sender.

Downloading files for player's preference is one of the utilities. To gain enough download flow, peers prefer to upload the good quality files to simplify the computation. We assume that all the downloading has the same preference coefficient, marked as $\omega_{pre} \geq 1$. If we assume the system time consists of many the same intervals of time, ΔT. Then we can compute the utility of a node a_i in its k_{th} phase ΔT_k. We write it as $u^1_{i,k}$ and get it from the formula:

$$u^1_{i,k} = \sum_{i\in GD} \omega_{pre} \bullet Q^{dl}_i \bullet SP^{dl}_i \bullet \Delta T_k - \sum_{i\in GU} Q^{ul}_i \bullet SP^{ul}_i \bullet \Delta T_k \,. \quad (1)$$

In terms of the P2P file sharing system game rules, the download flow is no more than the upload flow (the node contribution), i.e.

$$\sum_k \sum_{i\in GD} Q^{dl}_i \bullet SP^{dl}_i \bullet \Delta T_k \leq \sum_k \sum_{i\in GU} Q^{ul}_i \bullet SP^{ul}_i \bullet \Delta T_k \,.$$

So we can get $u^1_{i,k} \geq 0$. This is a motivate mechanism for participants to share their files.

The other part of utility is the nodes' reputation. It connects with the evaluation that happens at the end of a transaction. The user expresses his attitude to the quality of the exchanged file. If the comment were positive, the reputation value would add one, otherwise, subtract one. Let h be the reputation value, $h_{i,j}$ the value that a_i access a_j's files. The *trust value computation* is a function that maps the reputation value to a real interval (generally [0, 1]). If a peer has no transaction records about its opponent, it will collect the other's records (called indirect trust or recommend trust). The trust value computation expressed by a formula with different weight is composed of the direct transaction history records and the recommend trust value. It is similar to the following formula (2) that peer a_i computes the trust value of peer a_j:

$$CP_i = \omega_1 CP(h_{i,j}) + \omega_2 TR_k CP(h_{k,j})$$

where $\omega_{1,2}$ is weight, $a_k \in GD_j \setminus a_i$ (2)

Let $TR_{i,k}$ be a_i trust value in ΔT_k, the node trust utility is: $u^2_{i,k} = TR_{i,k} - TR_{i,k-1}$.

Consider the above mentioned, we can describe the P2P file sharing system with AATS as follows:

Definition 2 (Model of P2P file sharing system) is a tuple $M=(Q, Q_0, P, \pi, Ag, Ac, \rho, \tau, \Upsilon, \Sigma, \|\bullet\|)$. Where: Q is a non-empty set of states of the P2P file sharing system. Q_0: initial states. P: A finite, non-empty set of atomic propositions including the utility propositions. π: $Q \rightarrow 2^P$ is an interpretation function. Ag: $Ag=GAG$ is an agent set. Ac: the action set of the agent,{*GAC*}. ρ: $Ac \rightarrow 2^P$ is the action precondition function. τ: $Q \times Ac \rightarrow Q$ is a partial system transition function showing the result of the trusted node selection. Υ: The *strategy term* set enumerated above. Σ: Strategy set, composed by actions. $\|\bullet\|$: $\Upsilon \rightarrow \Sigma$.

Now, we introduce some predications into the model. The first is comparison predication *COMPARE(x,y)*, where $x, y \in \Re$. The semantic is comparing x with y, *COMPARE (x,y)* holds iff $x \geq y$. The second replacement predication is $REPLACE(ag_1, ag_2, act)$, where $ag_1, ag_2 \in Ag$, $act \in Ac$. It means peer ag_1 will execute the action *act* instead of ag_2. For example, $\langle\langle a_0\rangle\rangle \circ REPLACE(a_1, a_2, DLQ(Q^{dl}_i, a_0))$ denotes that a_0 chooses a_2 to replace a_1 and will download file with quality Q^{dl}_i from a_2 in the next step. The third predication is *SELECT(ag, group, rule)* , where $ag \in Ag$, $group \subseteq Ag$, *rule* is selection condition that *ag* satisfied.

III. Constraints and Deductive Rules in P2P Files Sharing system

A. The constraints of system

The system of file sharing must satisfy some constraints and user demands. These constraints guarantee the reasonableness of the system. Thus, we must discuss some constraints of demands like trust constraint. Formally, we represent them with atomic propositions or well-formed formula of atomic propositions.

（**a**） The game rule between downloading flow and uploading flow of file sharing system is:

$$\varphi(c_1) = \sum_k \sum_{i\in GD} Q^{dl}_i \bullet SP^{dl}_i \bullet \Delta T_k \leq \sum_k \sum_{i\in GU} Q^{ul}_i \bullet SP^{ul}_i \bullet \Delta T_k$$

It ensures that the rules of the game promote the node uploading. It means that a node can do the downloading operation only if the nodes have contributed to the system, that is to say, the download flow is no more than the upload flow.

（b） The constraint of Qos is:

$$\varphi(c_2)=(SP^{ul}_i \geq SP^{ul}_N) \wedge (SP^{dl}_i \geq SP^{dl}_N) \wedge (SP^{ul}_{i,MAX} \geq \sum_i SP^{ul}_i) \wedge (SP^{dl}_{i,MAX} \geq \sum_i SP^{dl}_i)$$

where SP^{ul}_N (SP^{dl}_N) is the minimization flow that Qos required, $SP^{ul}_{i,MAX}$ ($SP^{dl}_{i,MAX}$) is the maximization flow that peers can offer. The whole means the flows are more than Qos required and less than the ability of the system.

（c） Trust value is the foundation of judging the trust of the opponents. When a peer chooses its opponent, the trust value of opponent must larger than threshold TR_N. The trust constraint is:

$\varphi(c_3)= CP_i\ (h_{i,j}, h_{m,j}$ where $a_m \in GD_j \setminus a_i) > TR_N$

When these three constraints are satisfied, it is written as $\varphi(c_1) \wedge\varphi(c_2)\wedge\varphi(c_3)$ rather than all the formulas.

Potential risk is another consideration for peers to make decision. All the peers prefer less risk when they have the same payoff. The trust value suggests the quality of files. Thus, the risk of downloading and trust value is related. Higher trust value implies less risk of obtaining a low quality files. Let the risk function be $risk(x) \in [0, 1]$, where x the object being evaluated, there are two implications in the trust value.

$(TR_i \geq TR_j) \rightarrow (\langle\langle\ \rangle\rangle \circ SELECT(a_i, \{a_i, a_j\}), (risk(TR_i) \geq risk(TR_j)))$

$(TR_i \geq TR_j) \rightarrow (risk(TR_i) \geq risk(TR_j))$

B. The strategy deduction rules

To deduce the relationship between the reputation and the utility, we give some deductive rules in CATL. These rules show how the participants commit to the strategy according to utility. The peers compute the trust value of their opponents and select the strategy to maximize its benefit. The dominant strategy supports the peer to do so and simplifies the process of the selection.

Definition 3 (weakly-dominant strategy of single step) [20] if a_i chooses a strategy σ in state q, its expected utility is no less than what the alternative strategies do. Strategy σ is called weakly-dominant strategy of a single step, denoted as $wd_i(\sigma)$.

This rule provides a simple reason for strategy selection based on the theory that a rational agent will always play a dominant strategy. Let U_{next} denote the peer's utility set consisting of all the possible utilities when it chooses a different path. Then the rule is:

$$wd_i(\sigma)= \bigwedge_{u'\in U_{next}\setminus u_i} (\langle\langle a_i\rangle\rangle \bigcirc (u_i \geq u_i') \rightarrow C_i(\sigma, \langle\langle\ \rangle\rangle \bigcirc (u_i \geq u_i'))) \quad (3)$$

Example 1: In p2p file sharing system, a peer a_0 finds a_j has the file that it wants. Then a_0 decides whether the trust value of a_j is more than the threshold TR_N. If it's true, then the downloading starts. The description of CATL is:

$\langle\langle a_j\rangle\rangle \circ ((SCH(a_j) \vee (RC_0(a_i, a_j) \wedge (a_i \in NG)) \wedge \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3))$

$\rightarrow C_i(replace(a_j, \varphi, DLQ(Q^{ul}_{Expect}, a_j)), \langle\langle\ \rangle\rangle \circ (u_0 \geq 0))$

where NG is the neighbor group of a_0.

P2P peers will obey the rule if it predicted the next utility. It will select the state follow the rule. However, when antagonist selects its weakly-dominant strategy, this dominated state may not hold. Because of that, the rule (3) must be stricter. If a strategy can ensure the weakly-dominant strategy of a single step is held when the opponent chooses its own weakly-dominant strategy of a single step, the strategy is called weakly-dominant strategy of single phase.

Definition 4 (weakly-dominant strategy of single phase) if a_i chooses a strategy σ_i in state q, the strategy can ensure that $wd_i(\sigma_i)$ holds after the opponent a_j chooses its own weakly-dominant strategy σ_j at state $\lambda[1]$ for $\forall\lambda \in comp(\Sigma_i, q)$. Strategy σ_i is called weakly-dominant strategy of single phase, denoted as $Wd_i(\sigma_i)$. Then the rule is:

$$Wd_i(\sigma_i)= (C_j^{\lambda[1]}(\sigma_j, wd_i^{\lambda[0]}(\sigma_i)) \rightarrow \bigwedge_{u'\in U_{next}\setminus u_i} C_i^{\lambda[0]}(\sigma_i, \langle\langle\ \rangle\rangle \bigcirc (u_i \geq u_i'))) \quad (4)$$

The weakly-dominant strategy strengthens the selection condition without involving the long-run utility of the peers. If we considered the whole path of a peer, we could get the weakly-dominant strategy of sub-game.

Definition 5 (weakly-dominant strategy of sub-game) if a_i chooses a strategy σ_i in state q, for $\forall\lambda \in comp(\Sigma_i, q)$ and $n>0$, the strategy can ensure that $wd_i(\sigma_i)$ holds in each of the following state $\lambda[n]$. strategy σ_i is called weakly-dominant strategy of sub-game, denoted as $SWd_i(\sigma_i)$. Then the rule is:

$$SWd_i(\sigma_i)= \bigwedge_{n\in\mathbb{N}} (C_i^{\lambda[n]}(\sigma_i^{\lambda[n]}, wd_i^{\lambda[0]}(\sigma_i)) \rightarrow \bigwedge_{u'\in U_{next}\setminus u_i} C_i^{\lambda[0]}(\sigma_i, \langle\langle\ \rangle\rangle \square (u_i \geq u_i'))) \quad (5)$$

It is similar to definition 5 to define the "possible" dominant strategy.

Definition 6 (weakly-dominant strategy of expectation) if a_i chooses a strategy σ_i in state q, for $\forall\lambda \in comp(\Sigma_i, q)$ and $n>0$, the strategy can ensure that $wd_i(\sigma_i)$ holds in a state $\lambda[n]$. Strategy σ_i is called weakly-dominant strategy of expectation, denoted as $EWd_{i\ i}(\sigma_i)$. Then the rule is:

$$EWd_i(\sigma_i)= (C_i^{\lambda[n+b]}(\sigma_i^{\lambda[n+b]}, wd_i^{\lambda[0]}(\sigma_i)) \rightarrow C_i^{\lambda[0]}(\sigma_i, \langle\langle\ \rangle\rangle \Diamond (u_i \geq u_i'))) \quad (6)$$

These deduction rules are based on the node rationality and the utility maximization preference. Each node chooses the best strategy for its benefits in every state. The time costing will discount the expected utility because anyone wants to get the utility earlier so that he can gain more in the future. For this reason, we can conclude peers choosing the path according to time. Thus, there is a partial order in rules:

$$SWd_i(\sigma_i) \succ Wd_i(\sigma_i) \succ EWd_i(\sigma_i)$$

IV. "ADVERTISEMENT EFFECT" OF TRUST NODES SELECTION

Some properties that peers hold represent a trend of the system evolution. We analyze them in AATS and CATL to find out those factors of reputation system development. At last, we find there is a trend to exclude the new peers. We call this phenomenon as "advertisement effect".

To simplify the analysis of the P2P file sharing system, we propose the ideal model that tries to show what the peer would do with the trust constraint. First, we do some assumptions of ideal model.

Assumption 1: The peers in the system are rational, risk aversion, and non-cooperative with each other.

Assumption 2: The peers are honest, i.e., they cannot lie about their reputation record for TTP existing.

Assumption 3: The peers always use up the flow utility to download. Moreover, the upload and download are continuous, i.e. the flow appears in each phase and $Q^{ul}_i = Q^{dl}_i$.

In the ideal model, each peer wants to maximize its benefit and chooses its dominating strategy in each state. When a peer searches a file in the system, it will receive many results. For the expectation of the best quality file, peer often selects an opponent with highest trust value. Because of that, we will get proposition 1.

Proposition 1. Let strategy $\sigma = ((SCH(a_j) \vee (RC(a_i, a_j) \wedge (a_i \in NG)) \wedge \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3) \wedge select(a_j, GU, \bigwedge_{a_k \in GU \setminus a_j} COMPARE(TR_j, TR_k)))$, then $|= wd(\sigma)$.

Intuitively, we can prove the proposition in accordance with the best quality file with the highest trust value. We omit the proving procedure here.

From the view of the proposition 1, choosing highest trust value nodes is the weakly dominant strategy. The high reputation peers will be the first set selected by the others when downloading files.

The peers give their evaluation according to the file quality. Therefore, the reputation implies the results of comparing the quality of the files. Intuitively, the uploading flow relative to the inquired file should not be under the reputation influence. Unfortunately, we find it is not true. Relatively speaking, the utility of the upload behavior is different when the receivers do not have the same reputation. We will prove the next proposition before we study it.

Proposition 2. In the ideal model of P2P file sharing, the strategy σ_j of a_j is to be chosen first by its antagonist a_k when a_k select the download source. Then $|= wd(\sigma_j)$ *where* σ_j is

$$((SCH(a_j) \vee (RC_k(a_i, a_j) \wedge (a_i \in NG_k)) \wedge \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3) \wedge SELECT(a_j, GD_k, \bigwedge_{a_k \in GD_k \setminus a_j} COMPARE(TR_j, TR_k))))$$

Proof: Let Σ_k denote the strategy set of a_k, for $\forall \lambda \in comp(\Sigma_k, q)$. If a_j is to be chosen first by its antagonist a_k, there exists $v \in \aleph$ that satisfied

$\lambda[v] \;|= \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3) \wedge SELECT(a_j, GD_k, \bigwedge_{a_k \in GD_k \setminus a_j} COMPARE(TR_j, TR_m))$.

If not, $\bigwedge_{a_k \in GD_k \setminus a_j} COMPARE(TR_j, TR_k)$ =false. Let GD_k' denote the set of peers satisfied $\bigwedge_{a_m \in GD_k \setminus a_j} COMPARE(TR_m, TR_j)$. Let $a_m \in GD_k'$, then a_m is prior to a_j. So, a_j will be waiting until the peers in GD_k' are added in the source list of a_k. Then $\exists v' \in \aleph$ makes $\lambda[v'] \;|= \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3) \wedge SELECT(a_j, GD_k, \bigwedge_{a_k \in GD_k \setminus GD_k', a_j} COMPARE(TR_j, TR_k))$. We get $v' > v$, and in the sequence of λ, we get $\sum_{n=v}^{v'+1} \Delta T_n > \sum_{n=v'}^{v'+1} \Delta T_n$.

If a_j is at the first place, the expected utility of a_j is $u_j^{Expect} = \sum_{k=v}^{v+n} \sum_{i \in GU} -Q_j^{ul} \bullet SP_j^{ul} \bullet \Delta T_k$, where n is the sequence number of the time phases of uploading file. Otherwise, the expected utility is $u_j'^{Expect}$. For the assumption, the evaluation takes place after the downloading. Then $u^2{}_j$ will not change. The formula (1) reaches the maximum value when $Q_i^{dl} \bullet SP_i^{dl} \bullet \Delta T_k = Q_i^{ul} \bullet SP_i^{ul} \bullet \Delta T_k$. If $SP^{ul}{}_i$ and $Q^{ul}{}_i$ unchanged, we can get $u_j^{Expect} \geq u_j'^{Expect}$, that is to say:

$$\bigwedge_{u' \in U_{next} \setminus u_i} (\langle\langle a_j \rangle\rangle \bigcirc (u_j^{Expect} \geq u_j'^{Expect}) \to C_i(\sigma, \langle\langle\rangle\rangle \bigcirc (u_j^{Expect} \geq u_j'^{Expect})))$$

Then $|= wd(\sigma_j)$ □

From the proof of proposition 2, we can see that the reputation raises the expected utility. The reputation increment is a weakly dominant strategy for any peer in the file sharing system. For this reason, each peer has to upload more good quality files for pursuing good transaction records. It is one of the keys to prevent free-riding peers. We have a proposition deduced from proposition 2.

Proposition 3. In the ideal P2P file sharing model, peer a_i has to upload more good quality files to maximize utility in the limited time, i.e. a strategy of a_i is $\sigma = ((REQ_j(a_i) \wedge (SP^{ul}{}_{i,MAX} \geq \sum_i SP^{ul}{}_i)) \to (REPLACE_j(a_i, \varnothing, ULQ(Q^{ul}{}_i, a_i) \wedge ULS(SP^{ul}{}_i, a_i)))$, then $|= wd(\sigma)$.

One way to accumulate reputation is to offer support to more users. For the P2P files sharing model, the effect of the recommendation is another factor. However, that effect is not directly related. We have has a conclusion for that.

Proposition 4. In ideal model of p2p files sharing system, the strategy of peer a_j to select the peer a_i with higher reputation to upload its file is σ_j when there is a request array for downloading. Let $\sigma_j = ((REQ(a_i) \wedge (a_i \in GU_j) \wedge \varphi(c_1) \wedge \varphi(c_2) \wedge \varphi(c_3) \wedge SELECT(a_i, GD_i, \bigwedge_{a_k \in GU_i} COMPARE(TR_i, TR_k)))$, then $|= EWD(\sigma_j)$.

Proof: Let Σ_j denote the strategy set of a_j, for $\forall \lambda \in comp(\Sigma_j, q)$. If a_j answers the requisition of a_i first, $\lambda[0] \;|= \sigma_j$. Otherwise, a_j would possible be recommended. That is to say, $\exists v \geq 0$ and $a_k \in GU_j$ make $\lambda[v] |= \langle\langle a_i \rangle\rangle \lozenge RC_k(a_i, a_j)$. If the trust value TR_i of a_k is lower, assumed as TR'_i, i.e. $TR_i \geq TR'_i$, then $TR_i \cdot CP_i(h_x) \geq TR'_i \cdot CP_i(h_x)$, where $a_x \in GD_j \setminus a_k$, when formula (2) is used to compute the trust value of a_j. So the next formula is true.

$$(TR_i \geq TR'_i \to TR_i \cdot CP_i(h_x) \geq TR'_i \cdot CP_i(h_x),$$
$$\text{where } a_x \in GD_j \setminus a_k) \to TR_j \geq TR'_j$$

We get $|= wd(\sigma_j)$ in terms of proposition 2. Moreover, according to

$\langle\langle a_j \rangle\rangle C_j^{\lambda[v]}(\sigma_j, \langle\langle a_j \rangle\rangle \lozenge (u_j^{Expect} \geq u_j'^{Expect}))$ = True, where $C_j^{\lambda[v]}$ denotes a_j do the selection action in state $\lambda[v]$,

We can get

$$(\langle\langle a_j \rangle\rangle C_j^{\lambda[v]}(\sigma_j, wd_j^{\lambda[0]}(\sigma_j)) \to C_j^{\lambda[0]}(\sigma_j, \langle\langle a_j \rangle\rangle \lozenge (u_j \geq u_j')))$$

So $|= EWD(\sigma_j)$ □

Now, we can see that the peers would select more opponents with higher reputation if the peers want to get more benefit from the system. It likes advertisement process: the enterprises need numerous authority media to advocate their products to get more sale revenue. It is often a way to success. The phenomenon in P2P file sharing system is similar to this and we term it as "advertisement effect".

Unfortunately, "advertisement effect" does not help the system with improving. It blocks the new users because few peers in the system prefer to choose the newcomer so that many of them cannot get enough reputation. They would not receive the benefit without the uploading flow, which makes them organize the coalition to increase their reputation. On the other hand, the malicious peers take advantage of the advertisement effect to advocate each other, which known as Sybil attack.

To solve the first problem we need a good excitation mechanism to let the new one get enough reputation in a certain short period. To solve the second, there are two solutions for the collusion. The first solution is to recognize the coalition and deduce its trust as a whole. The second one is to consider whether the recommender is honest. Because "advertisement effect" depends on the higher reputation peers, we can raise the bar of recommendation ability so that the newcomer cannot recommend each other. Then the Sybil attack on reputation is restricted.

V. Trend of Small Files and Its Threat

The node selection strategy of a specified node is based on interest. The interest of a node in the model consists of two parts, reputation utility and actual utility. The relation between them, as we have analyzed, is that the reputation utility influences the actual utility through node selection. It is a fact that we calculate reputation by the evaluation of the historical interaction and the evaluation is based on the times of transaction. It raises a serious problem—nodes with different actual interest through different interaction traffic (often represented as the size of the file) can have the same reputation utility. This unfairness can cause imbalance in the reputation system.

We extend the meaning of the predicate *REQ* to inquiry of all the downloading files. Let *size*(*f*) be a function to denote size of file *f* and $f_{i,j}$ denote agent *i* has a file named *j*. The following proposition can be deduced.

Proposition 5. In a P2P file-sharing system, let σ_i be the uploading strategy of a_i that a_i uploads the file with least size first. If SP^{ul}_i is fixed and continuous and Q^{ul}_i is continuous: $((REQ(a_i)\wedge(a_j\in GD_i) \wedge\varphi(c_1)\wedge\varphi(c_2) \wedge\varphi(c_3) \wedge ULQ(Q^{ul}_i, a_i)) \wedge ULS(SP^{ul}_i, a_i)) \wedge ULF(SELECT(f_{i,j}, F_i, \bigwedge_{k\in\{1..n\}\setminus j} COMPARE(size(f_{i,k}), size(f_{i,j}))), a_i))$, then $|= EWd(\sigma_j)$.

Proof: Let Σ_i be the set of strategies of a_i. For all $\lambda\in comp(\Sigma_i, q)$, if a_i accepts a download requirement, a_i chooses to upload file in state $\lambda[0]$. Because SP^{ul}_i is fixed and continuous and Q^{ul}_i is continuous, u^1_i is same for each file that a_i chosen. For two files $f_{i,1}$ and $f_{i,2}$ with $size(f_{i,1})\leq size(f_{i,2})$, we have $size(f_{i,1})/ SP^{ul}_i \leq size(f_{i,2})/SP^{ul}_i$. If a_i's action of uploading $f_{i,1}$ is evaluated by his opponent in state $\lambda[v]$ and the action of uploading $f_{i,2}$ in state $\lambda[v']$, we get $v\leq v'$, i.e. a_i can be evaluated earlier by uploading a smaller file. In state $\lambda[v]$ a_i satisfies to $TR_i \geq TR'_i$. According to proposition 4 we have $|= wd(\sigma_i)$, i.e. $\langle\langle a_i\rangle\rangle C_i^{\lambda[v]}(\sigma_i, \langle\langle a_i\rangle\rangle\Diamond((u_i^2 \geq u_i'^2)\wedge(u_i^1 = u_i'^1))$ =True,

i.e.

$(\langle\langle a_i\rangle\rangle C_i^{\lambda[v]}(\sigma_i, wd_i^{\lambda[0]}(\sigma_i)) \rightarrow C_{ij}^{\lambda[0]}(\sigma_j, \langle\langle a_j\rangle\rangle\Diamond(u_j \geq u'_j)))$.

Therefore, $|= EWd(\sigma_j)$. □

Proposition 5 implies that a node is prone to choose small files to upload when the system is in stable state. With the absence of an efficient incentive mechanism, given that uploading small files produced sufficient payoff, a node would not upload large files even if there were high demands for large files.

In another word, reputation system induces "selfishness" since the payoff of a node consists of two parts. A node has different preferences upon traffic utility and reputation utility. We use the notation ω_u to denote the ratio of these preferences, i.e. $\omega_u = \Delta u_i^{1,\lambda[v]} / \Delta u_i^{2,\lambda[v]}$, $v\geq 0$. When $\omega_u\leq\omega_N$, a node is likely to choose traffic payoff that means the node will give up some of its reputation for more traffic when traffic payoff is sufficiently high. ω_N is called resistance coefficient that measures a node's ability of resistance to reputation loss regarding traffic payoff. We can define the type of nodes in a system in terms of resistance coefficient.

Definition 7 (Selfishness) In a P2P file-sharing system given $\omega_u(a_i) = \Delta u_i^{1,\lambda[v]} / \Delta u_j^{2,\lambda[v]}$, $v\geq 0$ and $\omega_N(a_i)$, which is the resistance coefficient of a_i, selfishness is a dominated choice strategy σ_i of a_i, $C_i(\sigma_i, \omega_u(a_i)\leq\omega_N(a_i))$

For a node who considers its own interests, the choice of selfishness is a priority to maximize its current interest.

Proposition 6 Selfishness is weakly dominated strategy, i.e. $|= wd(c_i(\sigma_1, \omega_u(a_i)\leq\omega_N(a_i)))$.

Proving procedure is omitted here。

Proposition 6 shows that the node will defect when the prospect of payoff is large enough. In designing a system, not only the possibility of the defection should be considered but also the detection of such defection.

Let Σ_i be the set of strategies of a_i. For all λ, $\lambda\in comp(\Sigma_i, q)$.

Let $\psi=\varphi(c_1)\wedge\varphi(c_2)\wedge\varphi(c_3)\wedge(Q^{ul}_i$ is good) $\wedge ULQ(Q^{ul}_i, a_i)) \wedge ULS(SP^{ul}_i, a_i)) \wedge ULF(SELECT(f_{i,j}, F_i, \bigwedge_{k\in\{1..n\}\setminus j} COMPARE(size(f_{i,k}), size(f_{i,j}))), a_i))$ denote that a node follows constraints and uploads small files with high quality.

$$\Psi' = \varphi(c_1)\wedge\varphi(c_2)\wedge\varphi(c_3)\wedge REQ(a_i) \wedge\left(\left(u_{a_i}^{1,\lambda[v+1]} - \sum_{j=0}^{v} u_{a_i}^{1,\lambda[k]}\right) / \left(u_{a_i}^{2,\lambda[v+1]} - \sum_{j=0}^{v} u_{a_i}^{2,\lambda[k]}\right) \geq\omega_N(a_i)\right)$$

The node satisfies to $\lambda[0]|=\langle\langle a_i\rangle\rangle\psi \cup \psi'$. when $\lambda[v]|=\langle\langle a_i\rangle\rangle\psi'$ a node chooses the selfishness strategy and earn a payoff of $u_i^{1,\lambda[v+1]} - \sum_{j=0}^{v} u_i^{1,\lambda[k]}$. Therefore, in the process of detection we have to recognize ψ' in $\lambda[v]$. The control over a node's payoff (e.g. the control that makes sure that traffic payoff is no larger than the sum of all previous contribution) can efficiently prevent that he defects in order to earn actual payoff.

There are two results from this pitfall that the files' real value is inundated by the evaluation of the node itself. It can cause the inequity of payoff in the process reputation calculation. One is the attack on networks caused by difference payoffs, called *difference payoff attack*. The other is Sybil attack that is the boost of reputation in a relatively shorter period by many small traffic transitions.

The first type of attack, according to the principle of KWRM, happens in the states just before the end of cooperation between nodes. Due to the enormous amount of nodes in a P2P environment the transition records cannot be completely kept. As time passes, the effect of negative reputation diminishes and finally disappears. Furthermore, a majority of positive reputation can inundate the few negative reputation that gives a node more traffic payoff, or vise versa. To handle such attack we can first keep malicious records for a longer time. On the other hand, when we evaluate the payoff of current transaction with a node, we keep checking $u_i^{1,\lambda[v+1]} - \sum_{j=0}^{v} u_i^{1,\lambda[k]}$ in order to be aware of the threat of defection that indicated by a sudden transaction amount, that is to say, we must supervise the opponent actual utility to conquer the defection.

The second phenomenon is a common problem in the current C2C e-commerce systems, e.g. e-bay and Tao-bao (in China), both of which evaluate reputation based on the amount of transaction. Even if there is a secure third party to keep the caution money, a node can still boost his reputation efficiently with a lot of cheap goods and cheats in selling the few expensive goods. When the monitor from a remote Trusted Third Party fails to function well the cheat can pull off. The most efficient resolution is to give a separate estimation for each goods of the service provider. However, this resolution demands huge amount of work. A more practical method is to categorize the goods according to their operating cash flow, i.e. the price of goods. C2C e-commerce systems suffer badly from Sybil attack because of low cost of Sybil attacks'. The categorization of cash flow can considerably increase the cost of Sybil attack and thus defend the attack more efficiently.

VI. CONCLUSION AND FUTURE WORK

In this paper, we analyze the reputation system in P2P files sharing model according to game theory and describe the model of P2P files sharing system by the logic language CATL based on AATS. We propose CATL and extend the deductive rules to study the rational peers in P2P system. The new rules are useful to analyze the trend of multi-agent system driven by trust and interest. CATL works well when we study the case of the P2P reputation system. With the new tools introduced into the P2P model, we study two pervasive phenomenons in P2P reputation system and name them as "advertisement effect" and "small-file-trend" respectively. In the future works, we will research on excitation mechanism for newcomers to find a good way to limit the recommendation abuse.

ACKNOWLEDGMENT

We gratefully acknowledge Wiebe van der Hoek for his help of understanding CATL. The financial of research is supported by the 863 program (2007AA01Z425, 2009AA012201), 973 program (2007CB316502), the National Natural Science Foundation of China(90718015), the joint of NSFC and Microsoft Asia Research(60970155), the Ph.D. Programs Foundation of Ministry of Education (20090072110035), the Program of Shanghai Subject Chief Scientist (10XD1404400), the State Key Laboratory of High-end Server & Storage Technology (2009HSSA06), the Fundamental Research Funds for the Central Universities (2008A039).

REFERENCES

[1] Y. Li, M. Zhou, Service Selection Approach Considering the Trustworthiness of QoS Data, J. Softw. 19 (2008) 2620-2627

[2] Y. Wang, J. Vassileva, Toward Trust and Reputation Based Web Service Selection: A Survey, Int. Trans. Syst. Sci. & Appl., 3 (2007)118-132

[3] D. Fudenberg, J. Tirole, Game theory, MIT Press (1991)

[4] S. D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The EigenTrust algorithm for reputation management in P2P networks, Proc. of the 12th Int'l WWW Conf. Budapest, ACM Press, (2003)640−651.

[5] X.Li, L. Liu, PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities, IEEE Trans. Knowl. Data Eng.,16 (2004) 843 – 857

[6] W. Dou, H. Wang, A Recommendation-Based Peer-to-Peer Trust Model, J. Softw. 15(2004) 571-583.

[7] A. Jøsang, E. Gray, Simplification and analysis of transitive trust networks, Web Intell. & Agent Syst. 4 (2006)139–161

[8] J. Zhang, X. Guo, Trust Evaluation Model Based on Fuzzy Logic for C2C E-Commerce, 2009 Int. Symp. on Inf. Eng. & Electron. Commer., IEEE Comput. Soc. Press (2009)403-408

[9] Z. Despotovic, K. Aberer, Probabilistic prediction of peers' performance in P2P networks, Eng. Appl. Intell. 18(2005) 771-780

[10] N. Liu, J. Li, Group-based Trust Model in P2P System Based on Trusted Computing, 2008 Int. Conf. on Comput. Sci. & Softw. Eng. Wuhan, IEEE Comput. Soc. Press (2008)797-801

[11] A. Jøsang, Touhid Bhuiyan, Optimal Trust Network Analysis with Subjective Logic, The 2th Int. Conf. on Emerg. Secur. Inf., Syst. and Technol., IEEE Comput. Soc. Press (2008)179-184

[12] A. Jøsang, R. Ismail, C. Boyd, A Survey of Trust and Reputation Systems for Online Service Provision, Decis. Support Syst., 43(2007)618-644

[13] W. Sherchan, S.W. Loke, A Fuzzy Model for Reasoning about Reputation in Web Services, Proc. of the 2006 ACM Symp. on Appl. Comput. Dijon, ACM Press(2006)1886-1892

[14] D. Artz, Gil. Yolanda, A survey of trust in computer science and the Semantic Web, Web Semant.: Sci., Serv. & Agents on the WWW, 5 (2007) 58-71

[15] M. Harish, G. S. Mahalakshm, Game Theoretic Model for P2P Trust Management, Proc. of the Int. Conf. on Comput. Intell. & Multimed. Appl. Sivakasi, IEEE Comput. Soc. Press (2007)564-566

[16] K. Komathy, P. Narayanasamy, Trust-based evolutionary game model assisting AODV routing against selfishness,

J. Netw. Comput. Appl., 31 (2008)446-471
[17] B. Mobasher, R. Burke, Toward trustworthy recommender systems: An analysis of attack models and algorithm robustness, ACM Trans. on Internet Technol., 7.(2007) Article No. 23
[18] W. Jamroga, N. Bulling, A Framework for Reasoning about Rational Agents, The Sixth Intl. Joint Conf. on Auton. Agents and Multi-Agent Syst., 3(2007)604-606
[19] R. Alur, T. A. Henzinger, O. Kupferman, Alternating-time temporal logic, J. ACM, 5 (2002)672–713
[20] W. v. d. Hoek, W. Jamroga, A Logic for Strategic reasoning. AAMAS'05, ACM Press, (2005)157-164
[21] V. Goranko, W. Jamroga, Comparing semantics of logics for multi-agent systems, Synth., 139(2004)241–280
[22] D. Walther, W. v. d. Hoek, Alternating-time Temporal Logic with Explicit Strategies, In D. Proc. of 11th Conf. on Theor. Asp. of Ration.& Knowl., (2007) 269-278.

Yu Bao, 1, 1, 1977, PhD student in the School of Computer Science and Technology of Tongji University, Shanghai, China. His research interests include authorization, trust negotiation, trust management in distributed and heterogeneous networks, and trust protocol verification.

He received an M.D. in School of Computer Science and Technology of China University of Mining & Technology. Contact him at baoyucumt@126.com.

Guosun Zeng, 1964, is a professor in the School of Computer Science and Technology of Tongji University, Shanghai, China. His research interests include authorization, trust management, trust protocol verification and model checking in distributed network.

He received a PhD in computer engineering from the University of Murcia. Contact him at gszeng@tongji.edu.cn.

.

Ke Zhang, 1975, is a PH.D student in the School of Environment science and spatial informatics, China University of Mining & Technology. His research interests include trust negotiation, distributed networks.

He received received an M.D. in Department of Computer Science and Technology of China University of Mining & Technology. Contact him at ZhangKe@cumt.edu.cn