A Distributed Decision-Making Mechanism for Wireless P2P Networks

Xu Wu, Jingsha He, Fei Xu, and Xi Zhang

Abstract: **Trust-based solutions provide some form of payment to peers to encourage good behavior. The problem with trust management systems is that they require prior knowledge to work. In other words, peers are vulnerable to attack if they do not have knowledge or correct knowledge of other peers in a trust management system. Therefore, considering only trust is inadequate when a decision is made to identify the best set of peers to utilize. In order to solve the problem, we propose a distributed decision-making mechanism for wireless peer-to-peer (P2P) networks based on game theory and relevant trust mechanisms in which we incorporate the element of trust and risk into a single model. The main idea of our mechanism is to use utility function to express the relationship between benefits and costs of peers, and then make the decision based on expected utility as well as risk attitude in a fully distributed fashion. The unique feature of our mechanism is that it not only helps a peer to select its partners, but also mitigates vulnerabilities in trust-based mechanisms. Through analysis and experiments, we believe our approach is useful for peers to make the decision regarding who to interact with. In addition, it is also a good starting point for exploring tradeoffs among risk, trust and utility.**

Index Terms: **Decision model, risk, trust, utility, wireless peer-to-peer (P2P) network.**

I. INTRODUCTION

Peer-to-peer (P2P) systems have gained tremendous attention of many researchers and companies. Each peer in a P2P system is presumed to have the equivalent functionality and is willing to share resources. Because of its ability to pool together and harness the large volume of resources, P2P systems' features include scalability, service availability, self-organization, fault tolerance, and load balancing. However, most P2P systems assume peers are using fixed Internet instead of wireless networks. Here we consider a mobile P2P network is an infrastructure designed to support mobile devices and wireless networks.

Mobile P2P Networks are also organized according to the P2P principle, they are autonomous (independent of any infrastructure), self-organized and decentralized. A mobile P2P network is a set of moving objects that communicate with each other via unregulated, short-range wireless technologies.

There have been many efforts dealing with security problem in P2P computing applications [1], [2]. The main research focus on security is dominated by trust-based solutions. Trust management approach for distributed systems security was first introduced in the context of Internet as an answer to the inadequacy of traditional cryptographic mechanisms. Some of the notable earlier works in this domain have been trust-management engines [3]. Since then, trust-based frameworks have been extensively studied in many contexts and equally diverse domains such as human social networks, e-commerce, 802.11 networks, peer-to-peer networks, etc. [4].

Trust management systems focus on accumulating trust values and propagating them through the network, so other peers can interpret the trust values to make decisions on who they should trust. The idea of constructing a trust-based scheme is motivated from existing human societies in the world. Embedded in every social network is a web of trust; with a link representing the trustworthiness between two individuals. When faced with uncertainty, individuals seek the opinions of those they trust. A similar trust management mechanism is developed for mobile P2P Networks, where peers maintain trust value for other peers. This trust value is used to evaluate the trustworthiness of other peers. This establishes a web of trust in the network, which is then used as an inherent aspect in predicting the future behavior of peers in the network.

However, current trust-based solutions [5]–[8] are vulnerable in the wireless P2P networks because they do not prevent attack, they just give more reason to cooperate in the system, but the vulnerability is still there if the malicious peer prefers acting maliciously enough. There are three main insufficiencies of trust-based solutions in wireless P2P systems.

Firstly, as the peers move around, the topology of the mobile P2P network changes dynamically. This makes trust overlay does not match with the physical network topology. Moreover the worse result is that a network may be separated into several disjoint "islands," where each "island" is completely disconnected from each other. The kind of scenario is named as network partitioning. It is difficult to build stable trust relationships between mobile peers based on current trust-based solutions.

Secondly, current trust-based solutions require prior experience in order to make decisions. As a result, a malicious peer must have previously attacked another peer in order to be recognized as malicious. In a foreign system with no known trusted peers, an entering peer is vulnerable to attack as it has no means to determine the trustworthiness of any other peers in the system. This fact can be exploited by an individual malicious peer or by a set of collaborating peers.

Thirdly, a mobile P2P network is also an abstract, logical network called an overlay network which builds on basic communication network, because there is no control of peers joining or leaving the network, a lot of drawbacks of the real mobile P2P systems have been disclosed. For example when a user tries

Manuscript received December 14, 2008.

X. Wu, J. He, and F. Xu are with the College of Computer Science and T technology, Beijing University of Technology, Beijing 100124, China, email: {wuxu, xf8878xf}@emails.bjut.edu.cn, jhe@bjut.edu.cn.

X. Zhang is with the Networking Technologies Department, Beijing Boren Jirui Company, Beijing 100099, China, email: xrdz2005@163.com.

using smart phone to download a file from another user's one, he may worry about the virus or attack embedded in that file. Since peers are heterogeneous, some peers might be benevolent in providing services. Some might be buggy or malicious and cannot provide services with the quality that they advertise [9]. Moreover, a peer can initially behave benignly, be recognized as such, and then act maliciously (either intentionally or due to being compromised). When it is found, the peer can reenter the network system by changing its network identity to get new reputation values in order to avoid the penalty imposed on it, which can't be identified from the fresh peers to the system by a trust management mechanism. Consequently, attack would happen when the malicious peer cheated in large interactions through improving trust value using many small interactions [10]. Since that peer would have a good trust value, a trust management system would give no reason not to trust that peer. This greatly hampers the implementation of the practical trust management system. These attacks are described as risks that require deeper investigation.

Therefore, considering only trust is inadequate when a decision is to be made in order to identify the best set of peers to utilize. Trust and risk have intrinsic relationship, i.e., trust is only meaningful in a risky situation. This is based on the original work by Deutsch [11] who laid the ground work on the notion of trust. Yet, in the current literature, few trust models proposed take risk into consideration. In fact, higher risk brings lower success rate of interaction. For example, Ajzen, in his theory of planned behavior, predicted that peers would be willing to interact if their perception of risk was low [12]. Thus, we believe that risk and trust are surely the crucial factors among many different factors for making a decision in an environment full of uncertainty.

In this paper, we propose a distributed decision-making mechanism for wireless P2P networks based on game theory and relevant trust mechanisms in which the element of trust and risk are incorporated into a single model. The main idea of our mechanism is to use utility function to express the relationship between benefits and costs of peers, and then make the decision based on expected utility as well as risk attitude in a fully distributed fashion. Our mechanism using game theory to model risk provides better protection from malicious peers, and defines the behavior of peers in a mobile P2P system by introducing utility function. The utility function takes into consideration the costs and benefits as perceived by each peer by being connected to the mobile P2P system and particular events that occur within the system. The aim of incorporating the element of trust and risk into a single model is to improve security in mobile P2P networks. The unique feature of our mechanism is that it not only helps a mobile peer to make a decision, but also mitigates vulnerabilities in trust-based security that are listed above.

Online route finding would be an example application where the proposed mechanism would apply well. For instance, Bob is visiting a new campus and wants to find the room where he is supposed to be giving a presentation from his current location, the University Center. He uses his PDA to contact a route service in the University Center, but is uncertain if the service is reliable (or even if it is malicious). He has several known routes on campus already stored in his PDA, so his PDA employs a decision mechanism in order to test the reliability of the service and reduce his risk of receiving bad results. In this case, the cost of making several requests is minimal relative to the cost of being attacked (going to the wrong building or room and missing her presentation), which is the type of application in which the proposed mechanism is most appropriate.

The rest of this paper is organized as follows. Section II presents the related work. Section III describes an overview of our proposed mechanism. Section IV contains the analysis of the proposed mechanism, and simulation results to its performance are expressed in Section V. Finally, Section VI gives conclusions and future work.

II. RELATED WORK

Trust-based solutions provide some form of payment to peers to encourage good behavior. The problem with trust management systems is that they require prior knowledge to work. In other words, peers are vulnerable to attack if they do not have knowledge or correct knowledge of other peers in a trust management system. As stated in the introduction, the vulnerability is most evident when a peer first enters a system or a peer previously recognized as benign chooses to betray trust (or is compromised). Therefore, considering only trust is inadequate when a decision is to be made in order to identify the best set of peers to utilize. In fact, higher risk brings lower success rate of interaction. We consider that peers would be willing to interact if their perception of risk was low.

In order to effectively solve decision problem of mobile P2P networks, we propose a distributed decision-making mechanism based on game theory and relevant trust mechanisms. Some existing trust management systems are introduced such as EigenTrust [5], PowerTrust [6], etc.

In the current literature, many trust models based on reputation have been proposed for P2P networks, for example EigenTrust [5], which is designed for the reputation management of P2P systems. The EigenTrust aggregates trust information from peer by having them perform a distributed calculation approaching the eigenvector of the trust matrix over the peers. In the model, the global reputation of peer i is marked by the local trust values assigned to peer i by other peers, which reflects the experience of other peers with it. The core of the model is that a special normalization process where the trust rating held by a peer is normalized to have their sum equal to 1. There are two main shortcomings in the model. Firstly, the normalization could cause the loss of important trust information. Secondly, EigenTrust relies on good choice of some pretrusted peers, which are supposed to be trusted by all peers. This assumption may be over optimistic in a distributed computing environment. The reason is that pretrusted peers may not last forever. Once they score badly after some transactions, the EigenTrust system may not work reliably.

Zhou and Hwang [6] proposed a power-law distribution in user feedbacks and a computational model, i.e., PowerTrust, to leverage the power-law feedback characteristics. The paper used a trust overlay network (TON) to model the trust relationships among peers. PowerTrust can greatly improve global reputation accuracy and aggregation speed, but it can't avoid the commu-

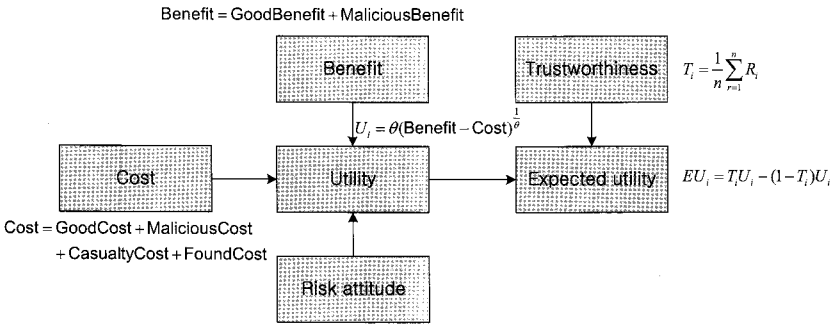

Fig. 1. Simplified overview of the decision model.

nication overhead in global trust computation.

Xiong and Liu propose a reputation-based trust supporting framework (PeerTrust) [4], which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system, and a decentralized implementation of such a model over a structured P2P network. PeerTrust model has two main features. First, it introduces three basic trust parameters and two adaptive factors in computing trustworthiness of peers, namely, feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the feedback sources, transaction context factor, and the community context factor. Second, it defines a general trust metric to combine these parameters. The limitation of this approach is that the computation convergence rate in large-scale P2P systems is not provided. The five factors used in their trust model must be retrieved with a heavy overhead.

Donato, Paniccia, and Selis [7] proposed new metrics for reputation management in P2P networks. The work combines these metrics with the original EigenTrust approach. The main contribution is that of introducing a number of new attack models not addressed before and a new metric called dishonesty.

A new trust model based on recommendation evidence is proposed for P2P Networks by Qi *et al* [8].

The proposed model has advantages in modeling dynamic trust relationship and aggregating recommendation information. It filters out noisy recommendation information.

The reputation-oriented trust issue is critical to e-commerce applications and has drawn much attention from both industry and the research community. Existing e-commerce systems have introduced trust management mechanisms that provide some rating information to customers. Lin *et al.* [13] review the reputation-based trust evaluation mechanisms in literature and outline some trust issues that are particularly important in e-commerce environments.

In this paper, we agree with such a viewpoint, that is to say, risk is one of the important factors that affect the decision making process. Recently, the relation of risk and trust has been discussed in different work [3], [14]. Presti *et al.* [3] provided an insight view of the relationship between trust and risk. They used the expected utility theory to model risk. But their model only concentrated on using risk to deduce trust rather than for making a decision regarding who to interact with. Our mechanism defines the behavior of peers in a mobile P2P system by introducing utility function. Research in game theory, has had a large influence in computer science. While much of the research is focused on auctions, some similar concepts that are discussed in this paper are being researched. In particular, economic-based approaches have permeated both security [2], [6] and P2P computing [1], [2]. These solutions do very little to address general malicious behavior in P2P systems. Instead, those related to P2P systems are largely focused on incentives to prevent freeloading. In the remainder of this paper, we borrow techniques from game theory in order to model risk in a P2P system.

III. OVERVIEW OF OUR MECHANISM

In the section, we give an overview of our proposed mechanism. Our mechanism incorporates the element of trust and risk into a single decision model in order to improve security. It defines a set of relationships between benefits and costs that are intended to capture the potential sources of benefit and cost that would drive a generic peer by introducing utility function. A simplified overview of our decision model expresses the relationships and main determinant factors that affect the decision making process in mobile P2P networks as shown in Fig. 1. We now define and briefly explain the main factors that we consider in our model.

Utility is a member of a set of input parameters that are used for constructing our decision model. In game theory, the usage of expected utility enables an agent to estimate the probability of winning the game. However, in many cases, the utility is not the same as monetary value and expected utility is introduced to express personal preferences. In classical utility theory, the expected utility can be expressed as a linear function of probabilities. In our mechanism, the utility function takes into consideration the costs and benefits as perceived by each peer by being connected to the P2P system and particular events that occur within the P2P system. A peer's actions will be evaluated based on its utility function.The utility function is normalized to unit-less (typically non-negative) values. Since most of the low-level components that make up the utility relationships are preferences, such as an aversion to being subjected to a denial of service attack, we do not provide any formal method for determining the values of those costs and benefits, though in many cases these benefits and costs could be described financially. Based on this nature, we incorporate the concept of utility and expected utility in our model, and use utility function to model

risk.

Trust is crucial for peers in such a distributed network environment. Lack of trust between peers is one of main challenges that obstruct the wide adoption of P2P systems. Trust has been examined in many contexts including sociology, social psychology, economics and marketing. Each context has a unique perspective on the notion of trust. In this paper, the notion of trust is that one believes and accepts the information which is provided by another in an uncertain and risky environment.Trustworthiness is the property of being able to be trusted while trust is to have the belief or confidence in the honesty, goodness, skill or safety of a person, organization or thing [16].

This means that trustworthiness is the property of being worthy of confidence [17].

Therefore, it is related to the reputation of a peer. The reputation is gotten based on its own experiences or a trust management system. The trustworthiness of a peer can be derived from its reputation. Our decision model can incorporate different methods to computer trustworthiness.

Risk attitude determines how much risk people can accept for moderate to large values of the probability of outcome or to avoid certain or highly probable losses. It also represents how willing a peer is to take risks, which depends on the character of an individual. There are different types of personal risk attitude such as risk averse, risk neutral and risk seeking. In this paper, the value of utility will be altered by the type of peer's personal risk attitude. The key reason to include this factor is because different peers usually have different tradeoffs between the expected utility and risk in mobile P2P networks. In traditional expected utility theory, the shape of the utility function determines risk attitudes as shown in Fig. 2.

In Fig. 2 the values or certainty equivalents, x, are plotted on the horizontal axis; utilities or expected utilities, u or $U(x)$, are on the vertical axis. You can use the plot of the function by finding a value on the horizontal axis, scanning up to the plotted curve, and looking left to the vertical axis to determine the utility.

A certainty equivalent is a certain payoff value which is equivalent, for the decision maker, to a particular payoff distribution. If the decision maker can determine his or her certainty equivalent for the payoff distribution of each strategy in a decision problem, then the optimal strategy is the one with the highest certainty equivalent. A utility function, $U(x)$, can be used to represent a decision maker's attitude toward risk. The certainty equivalent of the payoff distribution can be determined using the inverse of the utility function. That is, you locate the expected utility on the vertical axis, scan right to the plotted curve, and look down to read the corresponding certainty equivalent.

As noted, the above factors are closely related although the key factor is the expected utility that a peer has to consider and determine in each interaction. In the next section we analyze how these factors affect the decision-making process in such a distributed environment.

IV. ANALYSIS OF THE PROPOSED MECHANISM

We integrate risk and trust into a single model for peers to enrich the decision making process. In the decision model, peers

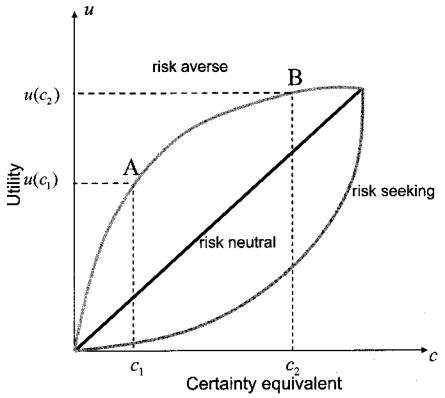

Fig. 2. The relationship between utility and risk attitude.

make an interaction decision by the evaluation of actions on potential partners based on the utility function as well as by their risk attitude. In this section, we describe the details of the decision model.

Consider a simple interaction scenario. A mobile peer is trying to download a file over the Internet. First, the peer will publicly announce its requested file in the mobile P2P network. The peers who want to provide the file then will send their request to the peer. Once the peer receives the response from all interested peers, it needs to make a decision of who to interact with. Let $M_1, \cdots, M_n$ be the set of peers who provide the file. C_i denotes the peer who is trying to download the file.

Currently, trust-based solutions are used in the decision- making process. However, the shortage with trust management systems is that they require prior knowledge to work. In the scenario the peer C_i is vulnerable to attack if the peer does not knowledge or correct knowledge of the peer M_i who provides the file in a trust management system. As stated in the introduction, the vulnerability is most evident when a peer first interacts with other peer in a system or a peer previously recognized as benign chooses to betray trust (or is compromised).

Therefore, considering only trust is inadequate when a decision is to be made in order to identify the best set of peers to utilize. In order to solve the problem, we propose a distributed decision-making mechanism for mobile P2P networks based on game theory and relevant trust mechanisms in which we incorporate the element of trust and risk into a single model.

The main idea of our mechanism is that we use utility function to express the relationship between benefits and costs as perceived by each peer by being connected to the P2P system and particular events that occur within the P2P system, and then make the interaction decision based on expected utility as well as risk attitude. In traditional expected utility theory [18], the shape of utility function determines the type of personal risk attitude.

Utility U_i is related to the personal risk attitude, and it can be defined as

$$U_i = \frac{1}{\theta}(\text{Benifit} - \text{Cost})^{\theta}. \tag{1}$$

In (1), the θ value is altered according to the types of personal

risk attitude [19]

$$\theta = \begin{cases} 1 < \theta \leq 2, & \text{if peer } C_i \text{ is risk seeking} \\ 1, & \text{if peer } C_i \text{ is risk neutral} \\ 0 < \theta < 1, & \text{if peer } C_i \text{ is risk averse.} \end{cases} \quad (2)$$

We can observe that peer C_i's risk attitude will change the value of utility. Compared to other types of risk attitude, risk seeking peers will tend to expand the utility more. On the other hand, risk averse peers prefer to reduce some utilities to avoid risk. U_i shows the relationship between benefits and costs as perceived by each peer by being connected to the P2P system and particular events that occur within the P2P system.Benefit is the payoff of peer which is gained in a P2P system. It is expressed as

$$\text{Benefit} = \text{GoodBenefit} + \text{MaliciousBenefit}. \quad (3)$$

Good benefit captures the benefit gained by legitimate participation in a P2P system. It consists of the benefit a peer perceives from sharing resources and any benefit that is derived from mechanisms in the system. Malicious benefit captures the benefit gained from acting maliciously. This is described by the actions of spying on a peer, denying access to a peer, and providing faulty information to a peer.

Cost is the expense of peer which is paid in a P2P system. It is denoted as

$$\begin{aligned} \text{Cost} =& \text{Good Cost} + \text{Malicious Cost} \\ &+ \text{Casualty Cost} + \text{Found Cost}. \end{aligned} \quad (4)$$

Good cost is the cost of participating in the system. This is the overhead cost of staying in the system (as derived and normalized from energy, memory, bandwidth, etc.) in addition to the costs incurred from providing resources and any costs from mechanisms incorporated in the system (such as punishments to prevent freeloading).

Malicious costs are costs associated with malicious actions, and include bandwidth costs or processing costs. While these are likely to be relatively small for a malicious peer, they do exist and are incorporated into the relationships. The Casualty cost is a relation that captures the negative effect on a peer when it becomes the casualty of an attack. It allows us to describe a peer's aversion to being attacked and plays a large role in determining how much effort should go into avoiding attacks or whether to participate in a system at all. Also included in the cost is Found cost which is the cost of an attacker being discovered (which may take the form of having to exit and re-enter the system or even just a decrease in available peers to attack).

In game theory, the usage of expected utility enables peers to estimate the probability of winning the game. Based on this nature, we introduce the concept of expected utility in wireless P2P networks. EU_i denotes the Von Neumann-Morgenstern Expected Utility for peer C_i. For the uncertainty of interacting, the expected utility EU_i of peer C_i is expressed as

$$\begin{aligned} EU_i &= pU_i - (1-p)U_i \\ &= p\theta(\text{Benifit} - U_i\text{Cost})^{\frac{1}{\theta}} - (1-p)\theta(\text{Benifit} - \text{Cost})^{\frac{1}{\theta}} \end{aligned} \quad (5)$$

where U_i is peer C_i's utility, and is expressed as the probability. We consider that the probability, p, of getting the interaction for the peer C_i is actually reflected by its trustworthiness. Based on this, the trustworthiness of a peer can be incorporated into (4). As the reader expects, the probability of getting the interaction for mobile peers is now correlated to the trust. Considerably, the more trustworthy a mobile peer is, the higher chance it gets the interaction when competing with a not-so trustworthy peer providing the same service.

The trustworthiness of a peer can be derived from its reputation, which is denoted as R_i. The reputation is gotten based on its own experiences or a trust management system. Our decision model can incorporate different methods to computer reputation. The trustworthiness of a peer can be expressed as

$$T_i = \frac{1}{n}\sum_{r=1}^{n} R_i \quad (6)$$

where n denotes the total number of interactions that peer M_i has conducted. As the probability p is related to trustworthiness, by rewriting the expected utility in (4), we get

$$\begin{aligned} EU_i &= T_iU_i - (1-T_i)U_i \\ &= T_i\theta(\text{Benifit} - U_i\text{Cost})^{\frac{1}{\theta}} \\ &\quad - (1-T_i)\theta(\text{Benifit} - \text{Cost})^{\frac{1}{\theta}}. \end{aligned} \quad (7)$$

In the paper, we define a set of relationships between benefits and costs that are intended to capture the potential sources of benefit and cost that would drive a generic peer. By generic, we mean that we do not require a peer to be purely malicious or purely benign. Instead, a peer's actions will be evaluated based on its utility function. The goodcost, mailiciouscost, goodbenefit and maliciousbenefit are used in the relationships. The utility function is normalized to unit-less (typically non-negative) values. Since most of the low-level components that make up the utility relationships are preferences, such as an aversion to being subjected to a denial of service attack, we do not provide any formal method for determining the values of those costs and benefits, though in many cases these benefits and costs could be described financially.

A mobile peer will make an interaction decision based on (6) and its risk attitude if it has knowledge or correct knowledge of the peer who provides the file in a trust management system, or else it will make the decision based on (1) and its risk attitude.

The risk averse peers prefer to have more protection than the profit. Thus, will always interact with the peers with the maximum expected utility among the trusted ones only. The risk neutral peers take a balance between two requirements. As a result, they always trade with the peers with maximum expected utility. Yet, risk seeking peers only focus on the utility gained. As a result, they always interact with the peers with the maximum utility regardless of their trustworthiness. In this case,

$$EU_i = U_i. \quad (8)$$

That is to say, for risk seeking peers, the providing peers with a high degree of trustworthiness and the deceitful peers will have

Table 1. Parameters used in the simulations.

Parameter	value
Communicating range	70 m
Simulation area	500 m × 500 m
Number of malicious peers	0%–70%
Risk attitude	averse, neutral, seeking
Communication protocol	802.11
Life time	50–100
Maximum speed	20 m/s

an equal interaction chance. Equation (7) shows that trustworthiness becomes meaningless while computing EU_i. After interacting is finished, the peers will use (5) to update the trust value of providing peer.

Similarly, a rational attacker would not find it beneficial to attack the peer if its MaliciousBenefit for the attack was less than what it expects based on the relationships between benefits and costs. Moreover if the malicious peer knows that the decision mechanism is being used, then it will have to probabilistically increase its benign service in order to not be discovered, which increases resource availability in the system and benefiting all benign peers.

V. SIMULATION RESULTS TO ITS PERFORMANCE

The objective of our experiments is to verify the effectiveness and benefits of our proposed mechanism. The simulation environment is set up as follows: We create 300 peers that will perform interacting in a mobile P2P resource sharing system. 300 mobile peers are uniformly distributed at the area whose size is 5000 m × 5000 m. Communicating range of a mobile device is 70 m.

The simulated experiments were run on a dual-processor Dell server and the operation system installed on this machine is Linux with kernel 2.6.9. To make our simulation as close to the real mobile P2P systems where peers often go offline, we simulate the offline peers by assigning every peer a random lifetime (or Time-To-Live) within the step range $[50, 100]$. After reaching the lifetime, the peer will not respond to any service request, and won't be counted in the statistics either. After one more step, the peer comes alive again with a new life time randomly chosen from the range $[50, 100]$.

In this analysis, we assume that all mobile peers have a same amount of battery power and participate in communication positively regardless of their roles. In the first experiment and second one, all peers participate 1000 rounds of interacting. In each round, each peer acts as both client and server to share its resources with other peers, and communicates with each other via IEEE 802.11. The default parameters in simulation experiments are showed in Table 1. Moreover in each experiment peers must follow the decision model through the whole interacting process. After completing the interaction, the involved parties update their trustworthiness of the other peers. Our results for some interesting cases are reported below.

In the first experiment we evaluate the mechanism in terms of the interacting success rate of peers with different risk attitude.

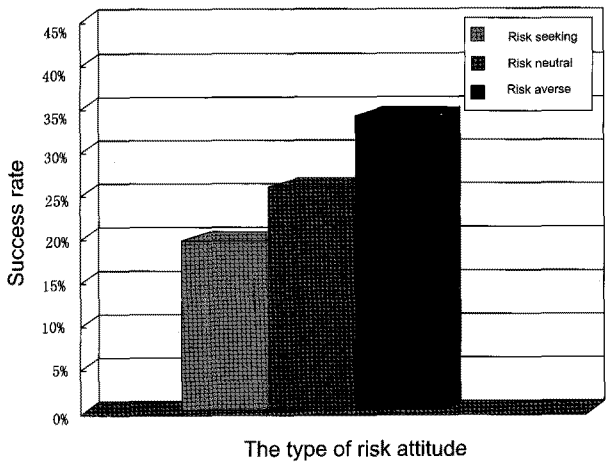

Fig. 3. The result of success rate.

Through experiments, we can see that during interacting, risk averse peers have the highest success rate (33%), risk seeking peers have the lowest success rate (19%) and risk neutral peers are in the middle (26%).

The experimental result expresses that the proposed mechanism can provide peers with more flexibility in the decision-making process, e.g., peers may decrease their benefits to get interaction chance. It is shown in Fig. 3 where the success rate is denoted as

$$\text{rate}(M_i) = \frac{\text{Success}(M_i)}{\text{Response}(M_i)} \times 100\%. \tag{9}$$

In (8), $\text{Response}(M_i)$ and $\text{Success}(M_i)$ denote the total number of responses and success that peer M_i has conducted. One main reason is the different risk attitude of peers. Peers with risk averse attitude tend to decrease their benefit to attract peers' attention in order to get the interaction chance. Moreover, they can also create more opportunities to improve their trustworthiness.

On the other hand, risk seeking peers would rather like to make more benefit according to the risk seeking level. The higher benefit is, the more probable it is for risk seeking peers to lose the interaction chance. They will become less competitive against other peers. Thus, Risk seeking peers appear to have the lowest success rate.

The second experiment shows how risk affects the changes of trustworthiness. As shown in Figs. 4–6, peers start with a trustworthiness value of 0.5. In Fig. 4, risk averse peers build up the trustworthiness by sacrificing part of the benefit due to the nature of personal risk attitude. In this sense, risk averse peers with poor trustworthiness will have chance to build up the trust. The same findings can be found in other peers with different risk attitude, Figs. 5 and 6.

This finding contradicts the traditional trust-based mechanisms where peers only interact with those that are known to be trustworthy. Since peers now consider the risk in partner selection, therefore, a peer with a low trustworthiness can make sacrifices of its benefit to get the chance of dealing with other peer.

In the case the peer would not find it beneficial to attack the peer based on our decision mechanism, so the malicious behav-

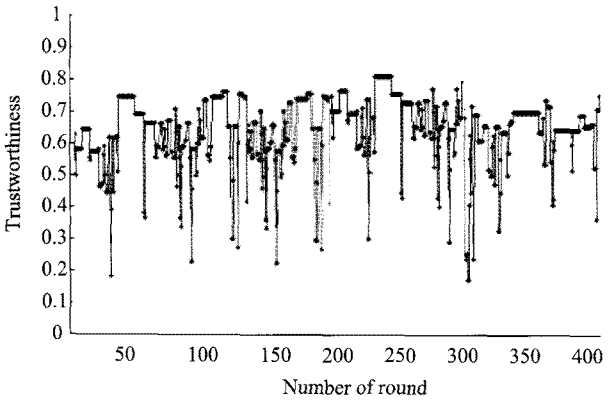

Fig. 4. Simulation results of peers with risk averse attitude.

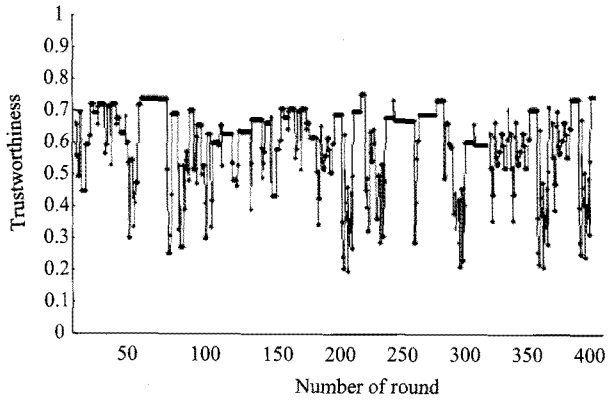

Fig. 5. Simulation results of peers with risk neutral attitude.

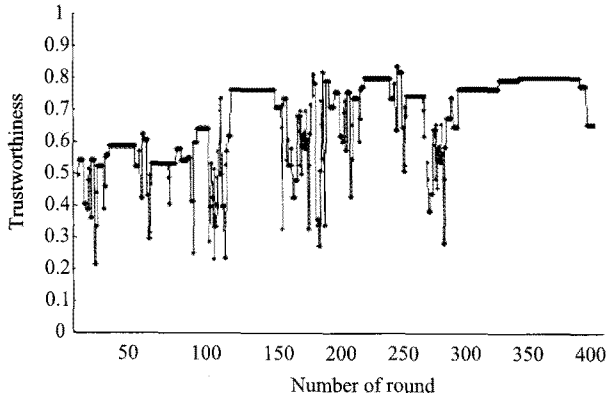

Fig. 6. Simulation results of peers with risk seeking attitude.

ior of peer is restrained in a certain degree. In addition, peers can interact with more than one peer in each round; therefore, it is normal to see that there are some "big jump" from high trustworthiness to low trustworthiness in Figs. 4–6.

In the third experiment, we assess the performance of our mechanism as compared to a mobile P2P resource sharing system where no decision-making mechanism is implemented. We simulate a network consisting of 300 mobile peers.

Results of experiment show that for risk averse peers and risk neutral ones, the proposed mechanism is qualified to prevent malicious peers' attacks while maintaining efficiency. The

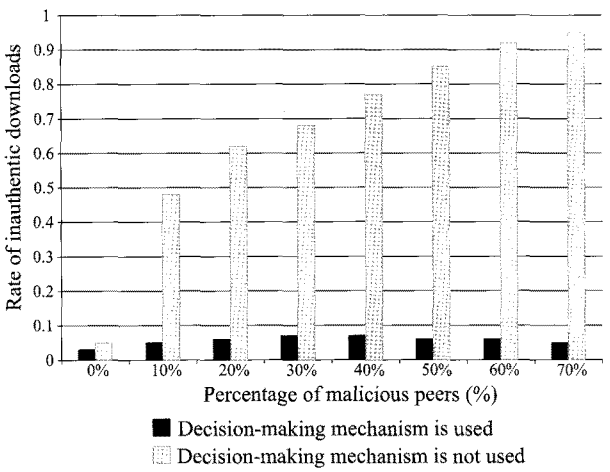

Fig. 7. Simulation results of peers with risk averse attitude under independent cheat.

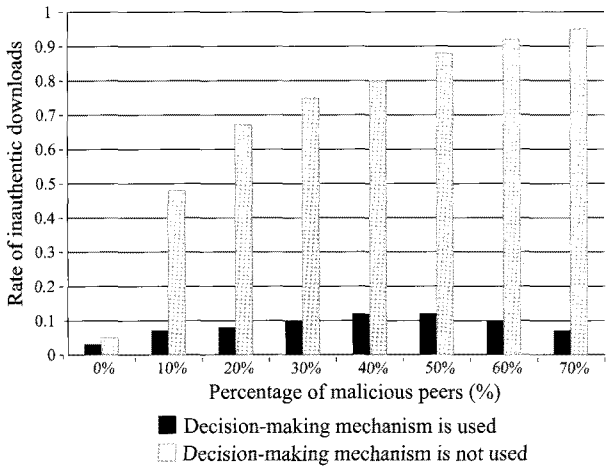

Fig. 8. Simulation results of peers with risk neutral attitude under independent cheat.

mechanism's performance is demonstrated under two attack models: Independent cheat and group cheat. Under independent cheat, the malicious peers firstly accumulate trust values through small interactions, gaining a relatively high trust. After trusted by most adjacent peers, the peer takes advantage of its high trust value to attack another peer, which means to always provide an inauthentic file to another peer when selected as download source. Group cheat is that there is a group in which the peer of the group provides an authentic file to each other and provides an inauthentic file to the peer outside the group.

We evaluate the mechanism in terms of the rate of inauthentic downloads of peers with different risk attitude. In each experiment, we add a number of malicious peers to the network such that malicious peers make up between 0% and 70% of all peers in the network.

For each fraction in steps of 10%, we run experiments under two attack models separately and depict the results in Figs. 7–12. In the absence of a decision-making mechanism, malicious peers succeed in inflicting many inauthentic download on the network under independent cheat and under group.

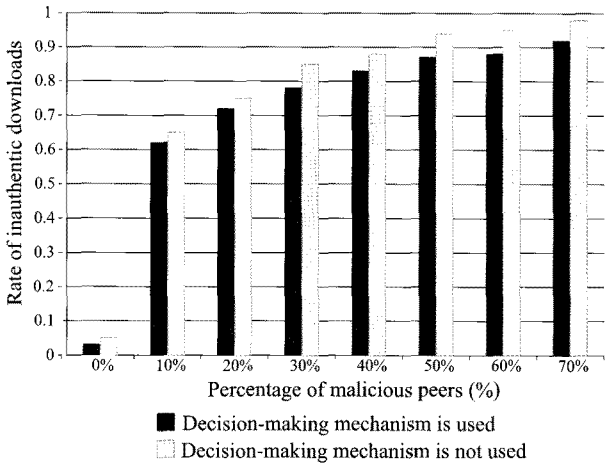

Fig. 9. Simulation results of peers with risk seeking attitude under independent cheat.

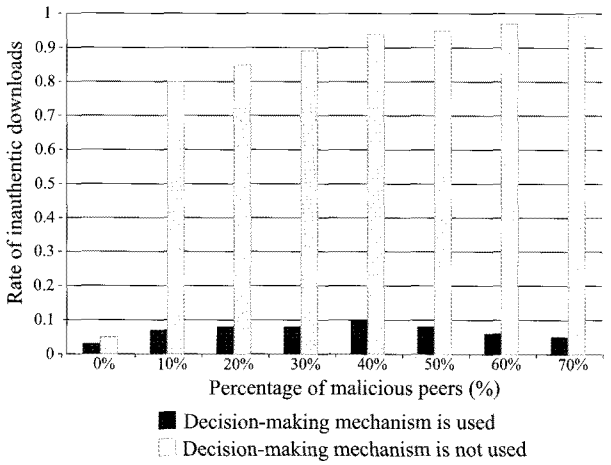

Fig. 10. Simulation results of peers with risk averse attitude under group cheat.

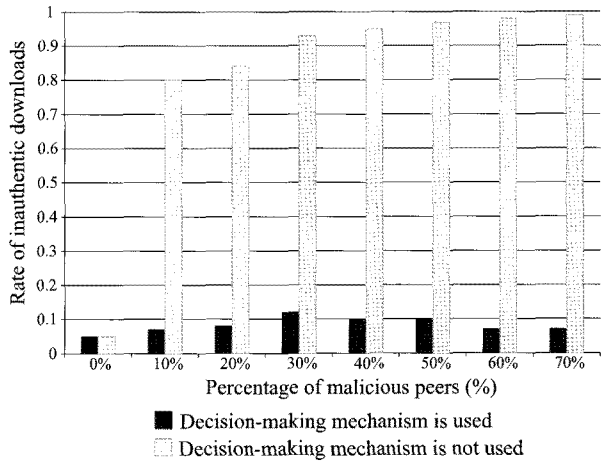

Fig. 11. Simulation results of peers with risk neutral attitude under group cheat.

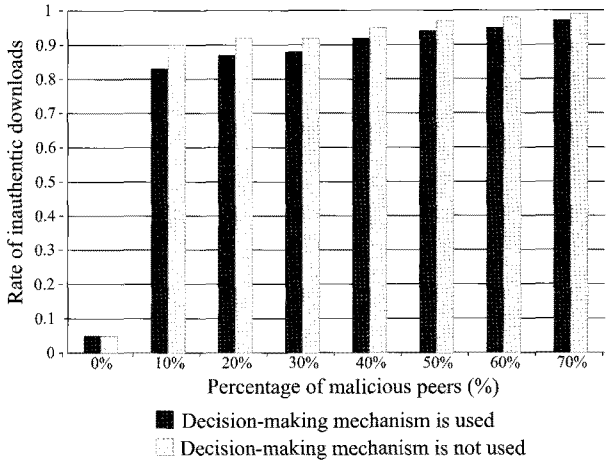

Fig. 12. Simulation results of peers with risk seeking attitude under group cheat.

However, for risk averse peers and risk neutral ones, our mechanism performs well even if a majority of malicious peers is present in the network at a prominent place. With our mechanism, a mobile peer will make an interaction decision based on (6) and its risk attitude if it has knowledge or correct knowledge of the peer who provides the file in a trust management system, or else it will make the decision based on (1) and its risk attitude.

Risk averse peers will always interact with the peers with the maximum expected utility among the reputable ones. Risk neutral peers have a balance between maximum profit and risk taking. So they always interact with the peers with the maximum expected utility. Thus, malicious peers are rarely chosen as download sources by risk averse peers and risk neutral ones, which minimizes the number of inauthentic file downloads in the system. We observed a 13% fraction of inauthentic downloads at most in Figs. 7, 8, 10, and 11.

Even if no malicious peers are present in the system, downloads are evaluated as inauthentic in 3%–5% of all cases—this accounts for mistakes users make when creating and sharing a file, e.g., by providing the wrong meta-data or creating and sharing an unreadable file.

The experiment results in Figs. 7, 8, 10, and 11 also clearly show that for peers with risk averse attitude and risk neutral one, forming a malicious collective does not decisively increase the rate malicious peers chosen as download source. Yet, risk seeking peers only focus on the utility gained. As a result, they always interact with the peers with the maximum utility regardless of their trustworthiness. That is to say, for risk seeking peers, the providing peers with a high degree of trustworthiness and the deceitful peers will have an equal interaction chance. So, the rate of inauthentic downloads of peers with risk seeking attitude is the highest. The simulation results of peers with risk seeking attitude are shown in Figs. 9 and 12.

These figures also show that risk averse peers have the lowest rate of inauthentic downloads, risk seeking peers have the highest rate and risk neutral peers are in the middle. In addition, an interesting fact is found in Figs.7, 8, 10, and 11. With our mechanism, the rate of inauthentic downloads of peers with risk averse attitude and risk neutral one firstly increases, then when the number of malicious peers increases to 30%–40% of all peers in the network, the rate starts to drop.

The reason is that the decision-making mechanism used in

our experiments punishes this behavior by lower the trust values quickly. Malicious peers found by the mechanism will lose choice selected as download sources. As a result, the rate of inauthentic downloads will drop. However, due to the collusion from the group cheat, the rate of inauthentic downloads under group cheap drops more slowly than the one in independent cheap. Yet one thing remains assured: The rate under group cheap is still dropping and drops to 3%–5%.

VI. CONCLUSIONS AND FUTURE

In this paper, we propose a distributed decision mechanism, and analyzed its usefulness based on utility functions of peers. The proposed unique approach is applicable to mobile P2P networks where peers roam into uncertain and unfamiliar environments. Our mechanism can be implemented individually without the cooperation of other peers in a system. As a result, it mitigates the problems inherent and often unaddressed by trust-based mechanisms. Furthermore, the proposed mechanism can provide peers with more flexibility in the decision-making process, e.g., peers may decrease their benefits to get interaction chance. We also discussed in this paper that peers with different personal risk attitudes can make decisions differently. Results of experiment show that for risk averse peers and risk neutral ones, the proposed mechanism is qualified to prevent malicious peer' attacks such as independent cheat and group cheat while maintaining efficiency. In the near future, we would like to test our mechanism into more real mobile P2P systems and analyze the system performances.

REFERENCES

[1] D. Figueirdo, J. Shapiro, and D. Towsley, "Incentives to promote availability in peer-to-peer anonymity systems," in *Proc. 13th ICNP*, 2005, pp. 110–121.

[2] M. Feldman, K. Lai, and I. Stoica, "Robust incentive techniques for peer-to-peer networks," in *Proc. 5th ECC/ACM ECC*, New York, USA, Oct. 2004, pp. 102–111.

[3] D. Donato, M. Paniccia, M. Selis, C. Castillo, G. Cortese, and S. Leonardi, "New metrics for reputation management in P2P networks," in *Proc. 3rd Workshop on Adversarial Information Retrieval on the Web*, Canada, May 2007, pp. 65–72.

[4] Z. Yan and P. Zhang, "Trust collaboration in P2P systems based on trusted computing platforms," *WSEAS Trans. Mag.*, vol. 3, pp. 275–282, Feb. 2006.

[5] X. Wu, J. S. He and F. Xu, "An enhanced trust model based on reputation for P2P networks," in *Proc. SUTC/IEEE*, Taichung, Taiwan, June 2008, pp. 67–73.

[6] R. Anderson and T. Moore, "The economics of information security," in *Science 314*, Oct. 2000, pp. 610–613.

[7] C. English, S. Terzis, and W. Wagealla, "Engineering trust based collaborations in a global computing environment," in *Proc. 2th iTRUST/IEEE iTrust*, Oxford, UK, 2004, pp. 135–145.

[8] M. Deutsch, "Trust and suspicion," *Conflict Resolution. Mag.*, vol. 2, pp. 265–279, 1958.

[9] S. D. Kamvar and M. T. Schlosser, "The eigenTrust algorithm for reputation management in P2P networks," in *Proc. 12th WWW*, Budapest, Bulgaria, May 2003, pp. 640–651.

[10] R. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted P2P computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, May 2007.

[11] I. Ajzen, "The theory of planed behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 197–211, 1991.

[12] J. V. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton, Princeton Univ, 1947.

[13] K. R. Gardner, *Games for Business ad Economics*, John Wiley and Sons, 1995.

[14] C. Q. Tian, S. H. Zou, W.-D. WANG, and S.-D. Cheng, "A new trust model based on recommendation evidence for P2P networks," in *Proc. Chinese J. Comput.*, Zurich, Switzerland, vol. 31, 2008, pp. 271–281.

[15] 2004. Cambridge dictionaries online. [Online]. Available: http://dictionary.cambridge.org

[16] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, pp. 843–857, 2004.

[17] Y. Wang and K. J. Lin, "Reputation-oriented trustworthy computing in e-commerce environments," *IEEE Internet Comput.*, pp. 55–59, 2008.

[18] A. Bieszczad, B. Pagurek, and T. White, "Mobile agents for network management," *IEEE Commun. Surveys*, vol. 1, Sept. 1998.

[19] 2005. Merriam-webster online. [Online]. http://www.webster.com

Xu Wu was born in Tonghua of Jilin Province in China. Currently, she is a Ph.D. student of Beijing University of Technology under direction of Professor Jingsha He, China's famous expert of computer technology. Her research interests include peer-to-peer reputation systems, overlay network design, Web services performance improvement, and trust and secure collaboration in mobile computing. She received her M.S. degree in Computer Science and Engineering from Beijing University of Technology, China, in 2005. Her thesis topic is scalable trust management systems for mobile peer to peer networks.

Jingsha He is currently a Professor of Beijing University of Technology in Beijing, China and the associate dean of the School of Software Engineering in the university. He received the B.S. degree in computer science from Xi'an Jiaotong University in Xi'an, China in 1982 and the M.S. and Ph.D. degrees from the University of Maryland at College Park, U.S.A. in 1984 and 1990, respectively. Prior to joining Beijing University of Technology in 2003, he worked for several technology companies such as IBM Federal Systems, MCI Communications and Fujitsu Laboratories of America doing research and development in the areas of computer networking and security. Prof. He's research interests include computer and network security, network measurement and wireless technologies, and his accomplishments include extensive publications, over twenty U.S. and China filed and granted patents, software copyrights, and authored books.

Fei Xu is a Ph.D. candidate of Beijing University of Technology. She received her Diploma and Bachelor degrees from the Shandong University of Technology in 2006. Her research interests are in the fields of network security, trust management, and privacy protection.

Xi Zhang is a software engineer. He works for Bei jing Boren Jirui company. His research interest includes networking security technologies and database management systems. At present, he is doing the research about wireless P2P Networks.