Inf Syst Front (2009) 11:43–60
DOI 10.1007/s10796-008-9148-6

Ubiquitous collaborative iTrust service: Exploring proximity collective wisdom

Yuan-Chu Hwang · Soe-Tsyr Yuan

Published online: 4 December 2008

Abstract Ubiquitous e-service is one of the most recent links in the chain of evolution that has characterized the different eras of the internetworking environment. In order to leap the trust barrier for the users to embrace these ubiquitous e-services, we present a collaborative iTrust e-service for exploring proximal collective wisdom in the ad-hoc ubiquitous environment. By highlighting the homophily of e-service participants, these isolated individuals can be treated as a group with proximity. Proximity thus enables ad-hoc e-service participants to contribute their strength for ubiquitous collective wisdom. Simulation outcomes for trust decision quality enhancement show significant improvement over traditional designs. The iTrust e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. It also facilitates and empowers the potential benefits of various ubiquitous e-service applications.

Keywords Ubiquitous e-service · Trust · Proximal collective wisdom · Ad-Hoc ubiquitous environment

Y.-C. Hwang (✉)
Department of Information Management,
National United University,
No. 1, Lien Da, Kung-Ching Li,
Miao-Li 36003 Taiwan, Republic of China
e-mail: ychwang@nuu.edu.tw

S.-T. Yuan
Department of MIS, National Chengchi University,
No.64, Sec.2, ZhiNan Rd., Wenshan District,
Taipei City 11605 Taiwan, Republic of China
e-mail: yuans@mis.nccu.edu.tw

1 Challenges for ubiquitous trustworthy e-Service

Current e-service applications focus more on centralized control aspect, where long-term historical data are collected and top-down design architectures are used to guarantee information service quality of e-service applications. Since Mark Weiser (1991) termed 'ubiquitous' as a new paradigm for computing in 1988, efforts have been concerted to develop and advance information technologies towards 'connecting, invisible calm and silent, and real' ubiquitous computing. The rapid growth of information systems technologies and networking has generated significant opportunities for streamlining decision-making processes and maximizing productivity through distributed collaborations. Emerging collaborative environments need to provide efficient support for seamless integration of heterogeneous technologies such as mobile devices and infrastructures, web services, grid computing systems, various operating environments, and diverse products. Such heterogeneity introduces, however, significant security and privacy challenges for distributed collaborative applications. In such a loosely-coupled open computing system, trust management has become essential, together with traditional cryptography techniques, for building a healthy collaboration among participating peers (or agents). Hence, ensuring trust in an ubiquitous environment is one of the most important tasks of the new networking paradigm. Recent work (McKnight and Chervany 2002) suggests that reputation based trust systems as an effective way for nodes to identify and avoid malicious nodes in order to minimize the threat and protect the system from possible misuses and abuses by malicious nodes in a decentralized overlay networks. Such systems typically assign each node a trust value based on the transactions it has performed with others and the feedbacks it has received.

However, the ubiquitous environment is different from a traditional static environment. It presents significant challenges for users in determining which users are trustworthy. In an ad-hoc ubiquitous e-service environment, since the ubiquitous identities are not designed for long-term lived and historical information is also seldom available in the ad-hoc e-service environment, previous solutions may not be applied to the ubiquitous environment. Environmental constraints and computational limitations make it more difficult to execute the process for determining which users are worthy of trust. There is no centralized or trusted 3rd party/agency to manage that task, and guarantee the trustworthiness of each identity. These new challenges complicate trust determination.

Since the ubiquitous e-service is highly correlated to user's current position, if the invasion of privacy is considered risky by users, users may resist the potential benefits of e-service. Since identities are short-lived, historical records may not available. Therefore, in an ad-hoc e-service environment that changes identity rapidly, there is little information available for others to determine whether users should be trusted. Without a trustworthy mechanism that can support user privacy protection and maintain transaction security, e-services may not attract enough participants to encourage e-services providers to enhance their service quality. By the same token, once the user perceives they are well protected from possible fraud or malicious transactions, the benefits of various e-service applications will increase significantly. This paper presents a collaborative iTrust mechanism to enable ubiquitous trustworthy e-service based on the proximal collective wisdom of the ad-hoc ubiquitous environment.

The remaining sections of this paper are organized as follows: In section 2, we review the literature about proximal collective wisdom and rationalize the use of the proximal collective wisdom for the iTrust e-service. In section 3, we describe the concept of the collaborative iTrust e-service which relies on the experience co-creation from proximal user groups. In section 4, we present the design concepts and the platform design of the iTrust e-service. We subsequently illustrate the evaluation results of the iTrust mechanism and discuss the significance and contribution of the iTrust design and the related works in Section 5. Finally, the conclusion remarks are provided in section 6.

2 Emergence of proximity for ubiquitous collaborative service

The ongoing developments of ubiquitous commerce have brought human life into a new era. Emerging ubiquitous e-service puts more emphasis on instantaneous interactions between e-service participants. Classic social science studies long ago demonstrated that proximity frequently increases the rate of individuals communicating and affiliating in organizations and communities (Allen 1977; Festinger et al. 1950). Proximity also develops strong norms of solidarity and cooperation. While advanced telecommunication technologies have led some to conclude that the problem of distance has been overcome, others argue that proximity remains essential to group functioning and that new technologies cannot eliminate the challenges faced by members of geographically-dispersed teams. The essentiality of proximity may be controversial, but the definition of proximity might change owing to technological innovations in the U-Commerce era.

The ubiquitous proximity e-service can be treated as a new scope of ubiquitous e-services that highlight the collective effort of proximity participants within a ubiquitous environment. Due to the dynamicity and complexity present in the ubiquitous world, it is unrealistic to expect humans to be able to reason and act effectively to address potential risks in the ubiquitous environment. In order to propose a new e-service paradigm that aims to mitigate potential risks and threats present in the ubiquitous e-service environment due to its flexible, dynamic, and collaborative nature, we will begin our discussion by considering the collaboration with proximal participants.

Sociologists and anthropologists have long recognized that people can feel close to distant others and develop common identities with distant others who they rarely or never meet. (Anderson 1983; Habermas 1991)Besides geographical distance, in the U-Commerce era, proximity places increased emphasis on individual homophily personal characteristics. The principle of homophily provides the basis for numerous social interaction processes. The basic idea is simple: "people like to associate with similar others." (Aristotle and Rackham 1934; Lazarsfeld and Merton 1954; Plato 1968) As mentioned above, ubiquitous proximity e-service stresses the collective efforts of participants in the dynamic environment. Homophylic user groups are more likely to combine the strength of different individuals to achieve specific objectives.

Homophily describes the tendency of individuals to associate and bond with similar others. By highlighting the homophily of e-service participants, these isolated individuals can be treated as a group with proximity (that is: common goals, similar interests, etc.). Interpersonal ties can be established in addition to some interactions. Loose-coupled e-service participants thus can be empowered to form groups/clusters with weak ties. Proximity thus enables ad-hoc e-service participants to contribute their strength for ubiquitous collective wisdom.

Since these ubiquitous e-service participants may also be unfamiliar with each other, it is necessary to integrate social

networks with trust issues in the ad-hoc e-service environment. However, a critical problem exists regarding trust decisions for strangers, "Why individuals should share information with strangers in an unfamiliar environment?" This problem involves problems of both interpersonal trust and efficiency. Relying solely on fixed Internet it is impossible to establish such extensive interpersonal trust networks in an ad-hoc e-service environment.

It is difficult for users to collaborate with complete strangers. No collective wisdom can be established in environments in which participants are completely isolated. A significant value of the proximity e-service lies in the increased possibility of establishing innovative social network relationships. From the interpersonal perspective, unfamiliar strangers can make connections with individuals who are proximal and homoplastic to him (that is, shared interests cause users to gather at a single exhibition). The strength of proximity gives people better chances to make interpersonal connections, including both weak ties (i.e. someone you know each other) and strong ties (i.e. good friends).

To solve the problem of creating trust in the ubiquitous environment, we propose the notion of collaborative trust e-service for exploring the collective wisdom in the ubiquitous environment, called "iTrust". An iTrust e-service is an ubiquitous e-service application that may obtain value-added information through the interactions of surrounding environments and/or users. An iTrust e-service allows users to choose and cooperate with trustworthy partners for executing transactions in the risky ubiquitous environment. The iTrust design integrates the concept of privacy protection, reputation management, and trust estimation in the ad-hoc ubiquitous environment. It is proposed to provide a feasible solution for quality decisions in the dynamic and distributed environment in which identities are short-lived and the computational abilities of mobile devices are limited. The notion of iTrust e-service highlights the collective effort focused on collecting the user group's power as the reference for ubiquitous trust decisions.

3 The concepts of the collaborative iTrust e-Service

Unlike the client/server commercial environment in which centralized databases or 3rd parties manage all trust related information, the only available information sources are from users themselves and the people around them. The major benefit of ubiquitous proximity e-service is based on the collective effort, by combining everybody's strength to build up a trustworthy environment that respects security, privacy and encourages the convenience of exerting mobile peers' e-service in the vicinity.

Since there is no authorized information sources in the ad-hoc ubiquitous e-service environment that guarantee which identity is trustworthy, the decision must rely on the users themselves. The iTrust e-service highlights the collaborative power to eliminate potential risks and provide appropriate estimation for trust decisions. Various kinds of available information may increase the heterogeneity and raise the system loading especially for mobile devices with a limited computational capacity. Increasing information heterogeneity implies complex computation, but it also creates significant collaborative power. According to Govier (1997), social trust is not blind, but derives from personal or interpersonal experience, and those experiences are gathered from the informal groups that constitute our daily life. Users may retrieve various experiences as the decision resource, but how are those experiences obtained from the ubiquitous e-service environment?

3.1 Experience co-creation approach

Experience co-creation occurs when users perceive powerful events from interaction experiences with other users. Reputation estimation is performed by aggregating these perceived experiences. For most commercial scenarios, reputation data is defined as transaction-based experiences. That is, when a transaction process is executed, reputation data will be established and recorded. Whether the transaction process is completed or abandoned, a reputation record from the transaction will still be generated (abandoned transactions usually have a negative effect on reputation). If reputation data is accessible, others may also take reputation data into their decision considerations. Experience co-creation in the iTrust e-service highlights the co-creation process and the shared experience of collective effort, which provides meaningful information for collaborative interactions.

In an unknown environment, users may not be familiar with the other people around them. They may not understand who is reliable or trustworthy. There is rare information available for trust decision in an ad-hoc ubiquitous environment. The iTrust e-service extends the information sources from traditional commerce scenarios that consider the transaction-based experience only. Instead, interaction-based experiences are considered as another heterogeneous data source.

Researchers have defined trust as an expectation. The expectations and determinations for trust are all related to the concepts of competence, benevolence and responsibility. Those are the major factors for satisfying the "Cognitive-based trust" and the "Affective-based trust" in interpersonal trust (Lewis and Weigert 1985; McKnight and Chervany 2002). When applying emotional measurement factors to judge provided services, interaction-based

experiences are desirable information sources for trust estimation—the judgment of whether the service provider has the ability to give the needed service. Does the buyer can comprehend whether the service provider really cares for their needs in providing the service? More importantly, do the provided services actually fulfill the buyer's urgent needs for all requirements? Table 1 indicates how those emotional factors are used for trust measurement in related research. The interaction-based trust is unfolded into those three the concepts as an alternative information sources. In addition to personal experience, available information sources also include the interpersonal experiences from one's social network. Heterogeneous interaction-based trust estimations are collected from the proximal user groups which represent experience co-creation process for contributing the collaborative trust decisions.

3.2 Collaborative trust estimation

In order to deal with the changes originating from the ad-hoc ubiquitous e-service environment, the solution must explore other possible data sources in addition to the transaction-based information, and seek out alternative evidences for trust estimation. However, experience data obtained from the surrounding environment or evidence chains over the social network may entail risks. If the obtained information cannot provide enough reliable evidence for better trust estimation results, then the tradeoff between data usability and efficiency should be taken into consideration. Since all of the available trust experience and other heterogeneous information sources should be taken into account for trust estimation, the limitations of mobile devices make the selection for comparative valuable information sources an important issue. Users have to decide the level of risk they are willing to endure from weighted heterogeneous data sources.

In the iTrust platform (i.e., an iTrust-enabled mobile device), a credibility investigation module is designed for experience sharing collaboration. Detailed descriptions of iTrust components are illustrated in the Section 4.2. After the credibility investigation process is completed, users may have the possession of three types of information sources for trust estimation. Including:

- Personal interaction-based experience from self-owned interaction pseudonyms. (Personal Local Trust, **PLT**)
- Interpersonal interaction-based experience from credibility investigation. (Nearby Peer's Local Trust, **NLT**)
- Transaction-based global reputation for specific target peer. (Global Reputation, **GR**)

The interaction-based experience estimation involves two dimensions. The first requires determination of the trustworthiness from the interactions by demander (customer) to justify whether the provided service satisfies their expectation. The second is responding to the credibility investigation by consolidation of the available personal experience as a trust evaluation value and send back to the investigation demander.

The determination of how a peer can recognize whether the various received service package information will satisfy user expectation will involve the cognitive-decision for each communication message. In order to facilitate mutual understanding for each peer, an ontology is essential for effective communication. In our study, the ontology-based search has great potential to facilitate the interaction parties matching their desired resources and comparing the received service package information in order to determine the candidate service provider. The fitness will be matched by comparing the demanded task and supplied services. Utilizing an ontology-based search for task matching can understand how the service provider understands the customer's needs and determines which service packages are the best candidates with highest fitness.

Users may have various needs and reliability concerns for different information sources, these heterogeneous sources may be applied with different importance for the user's final decision. The balance between heterogeneous information sources can be adjusted in the iTrust Profile Management module. The following three weighted parameters are used for the sake of aggregating heterogeneous information sources as the final score for trust candidate decision. WPLT represents the weight of personal interac-

Table 1 Interaction-based trust: definition concepts and related works

Concepts	Operational definition	Related work
Competence	Sellers should have the ability and have enough service resources for providing users their desired services.	(Earle and Cvetkovich 1995; Lewis and Weigert 1985; Mayer et al. 1995; McAllister 1995; Singh and Sirdeshmukh 2000)
Benevolence	Seller should really care about the customer's urgent needs and supply them appropriate services	(Lewis and Weigert 1985; Mayer et al. 1995; Singh and Sirdeshmukh 2000)
Responsibility	Provided services satisfy the original expectation.Service provider is able to reach the goal they promised to accomplish.	(Earle & Cvetkovich 1995; Lewis and Weigert 1985; Mayer et al. 1995; McAllister 1995)

tion-based experience from self-owned interaction pseudonyms. WNLT represents the weight of interpersonal interaction-based experience from credibility investigation. WGR represents the weight of transaction-based global reputation. The final score computation for trust candidate selection is shown as formula (1).

$$Trust_{FinalScore} = \frac{W_{PLT} \cdot PLT + W_{NLT} \cdot NLT + W_{GR} \cdot GR}{W_{PLT} + W_{NLT} + W_{GR}} \quad (1)$$

The final score for trust candidate selection represents the aggregate results from obtained heterogeneous data sources. A higher score means the information source is more trustworthy. A risk parameter β is also set up by the user in the User Profile as the trustworthiness threshold. Once the $Trust_{FinalScore}$ is lower than β, the corresponding interaction pseudonym is removed from the transaction candidate list. The best candidate will be the first priority for further service exchanges.

4 iTrust e-Service design

We have identified the major challenges in an ubiquitous environment and the urgent needs for collaborative iTrust e-service. We use the iTrust platform that considers privacy design, reputation management, and trust management as the central concepts for establishing an autonomous trust model for exploring the collective effort in the ubiquitous environment.

Different from traditional architecture, the iTrust e-service highlights distributed peer-to-peer interaction under ad-hoc network composition, and accommodates the dynamic short-lived identity characteristics and the limited computational capacities of mobile device. Also, the iTrust e-service provides seamless unlinkability to ensure user protection and adopts heterogeneous data sources to enhance quality for trust collaboration. Classical method designs may be used for partial solutions to the problem, but require heavy computations that are difficult to carry out in a mobile device. But most previous designs cannot be applied to our problem as their architecture is not suited to an ad-hoc ubiquitous environment and their design concepts do not address the challenges of the ubiquitous environment.

4.1 iTrust privacy and security design

The privacy protection design of iTrust is illustrated in Hwang and Yuan (2007). The iTrust privacy design concept is based on multiple layered pseudonyms to ensure identity security and unlinkability. The iTrust privacy design excludes a unique personal pseudonym for interactions to protect users from possible tracking and profiling. It uses multiple interaction pseudonyms to enhance the complexity of identity tracing by abstracting the design of role/relationship pseudonyms for service version selection and delivery. (i.e. versioning the services by specific types for performance consideration.) For transaction security, iTrust design uses a transaction pseudonym to ensure safety for a one time payment.

Before any interactions can be executed, peers require an identity for the service environment. We use the Interaction Pseudonym as an agent identity for the user. It should be noted that a user may possess several different agents for various e-services. An agent's identity is produced according to the service. A user can activate an agent identity or discard a specific identity based on their needs. Even if the user has many agent identities, all identities still share the same global reputation data. When an identity is created, it inherits the concurrent reputation from user's global reputation data. The reputation data for each identity does not exist separately. No matter how many identities belong to the user, he can keep only one global reputation. The diagram (Fig. 1) represents the general design concepts and the relationships of three kinds of pseudonyms. Only the Interaction Pseudonyms appear in the interaction environment. Interaction pseudonyms are generating through the same Active Pseudonym but without any linkage relationship. Interaction pseudonyms are cost-free (i.e. cheap pseudonyms); user can generate/discard them freely. However, user can not change their active pseudonym without cost.

4.2 iTrust platform

The iTrust e-service platform and its function modules are depicted in Fig. 2

4.3 Profile management

In the iTrust e-service platform, mobile users can manage their profile settings through a friendly user interface. The

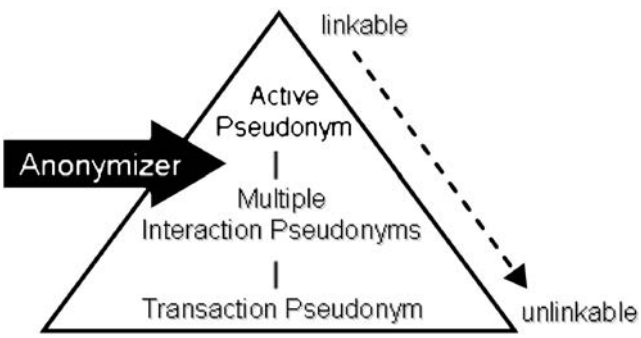


Fig. 1 A multiple layered pseudonym design for privacy protection

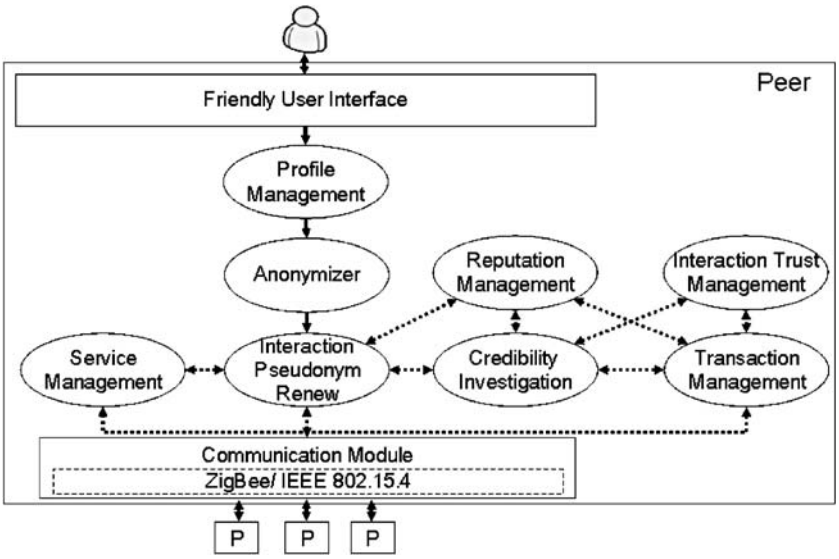


Fig. 2 Macro view of the Collaborative iTrust platform

profiles includes their preferences and the roles they would like to play, and various attributes such as user's willingness to participate, the will to disclose their interaction experiences, the risk level they can tolerate, and the reliability threshold for determining whether to interact with nearby peers. Once an identity has been generated, those settings will be assigned to the interaction pseudonym automatically.

4.4 Anonymizer

In the iTrust e-service platform, all interactions within the ubiquitous e-service environment are using the "Interaction Pseudonyms" instead of user's real identity or personal pseudonyms. The main function for the Anonymizer is to generate diverse occasional interaction pseudonyms based on their given identity for various kinds of e-services. Those interaction pseudonyms are valid for a short period, and are localized to the corresponding e-service acquired. Because the randomized interaction pseudonyms are not linked to real personal identities and are valid for a limited range, others will be unable to trace their real owner via the interaction pseudonyms. Those interaction pseudonyms are generated by the Anonymizer and will inherit the attribute parameters automatically through the Profile management module. They are able to execute the versioning process and cope with the service management module to reduce irrelevance transmission and improve the efficiency of interaction.

4.5 Interaction Pseudonym renew

As mentioned in previous sections, iTrust e-service has overcome the problem of the dynamic composition of surrounding peers that may change rapidly. The Interaction Pseudonym Renew module is used to update the list of current nearby users, which exhibits all available nearby peer interaction pseudonyms. Users can interact with peers around themselves through the Communication module. The Interaction Pseudonym Renew module is connected with the Reputation Management module, which may immediately update the global reputation of peers so that all devices in range may access it. Each exchange and transmission within the Service Management module, as well as information inquiry when performing credibility investigation, is targeted to those identities obtained by Interaction Pseudonym Renew module.

4.6 Service management

Service management in the iTrust e-service platform includes two major interactive function modules: the "Acquire sub-module" that acquires service and forwards peer requests to nearby peers within the e-service environment; and the "Acknowledge sub-module" that responds to or acknowledges the service request received from surrounding peers. Both of the sub-modules are equipped with a matching function that facilitates the assessment for service information exchange. The Acquire sub-module gathers all the responses provided by nearby peers who receive a user's request. Those responses include service package information offered by nearby service providers. For further interaction or transaction decisions, the reputation data of those service providers are also attached to the service package information, shown as a received service list. The Acknowledge sub-module complements the Acquire sub-module. After receiving the requests forwarded by nearby users, service providers can take into account their own behavior style settings and determine appropriate responses. Service providers may decide to

provide services identical to those of the request, or offer a substitute. After consulting the requester's public attributes, a suitable service package is created. The service package information attached with provider's reputation is delivered to the requesting peer through the Communication module. If the received services match the requesting peer's needs, the peer can decide follow-up interactions based on their perishability, or degree of urgency. In urgent situations, users may execute immediate transactions directly to those candidates, which will link to the Transaction module. Otherwise, they can obtain the trustworthy analysis result via the Credibility Investigation module for advanced decision-making.

4.7 Credibility investigation

By comparison with current mobile e-services, there may be little available data for credibility and trust estimation of unfamiliar users due to the natural limitations of ad-hoc ubiquitous e-services. In the iTrust e-service platform, the traditional transaction-based experience is considered for decision-making, along with the interaction-based experiences. For credibility investigation, there are two information sources available. The first source is similar to the current e-service's global reputation but without the linkage to the user's personal identity or detailed transaction histories. The second source is exploration of the collective effort of the social network and its most recent interaction experiences. Empowered by the characteristics of iTrust e-service, investigated data are concurrently updated and highly related to their location at the moment. After consideration of the various heterogeneous data sources against the user risk tolerance setting in the Profile Management module, the Credibility Investigation module filters out credible candidates for further transaction management.

4.8 Transaction management

After the user has determined the target peer for transaction, a transaction pseudonym is created automatically in the iTrust e-service platform. This transaction pseudonym is put to use for the payment process, which is also unlinkable to the user's real identity. That is, the transaction pseudonym is only valid for the specific service transaction for that period of time. Next, the reputation management module is launched to update the global reputation's of both seller and buyer.

4.9 Reputation management

Once the users have accomplished the transaction, a reputation evaluation token is exchanged. According to the feedback result recorded in the reputation evaluation token, the summarized global reputation data is updated automatically. The reputation evaluation tokens are blind-signed and enable unlinkability for keeping the reputation data from revealing the referee's true identity. This Reputation Management module not only acts as the information source for credibility investigation, but is also linked to the Interaction Pseudonym renew module for global reputation updates.

4.10 Interaction trust management

In contrast to the reputation management module that records the transaction histories, the interaction trust management module places emphasis on a user's direct interaction experience. It highlights the perceived value from the interaction's target peer and treats the interaction-based experience as another vital information source. In cooperation with the Credibility Investigation module, it provides heterogeneous information based on user experiences stored in the social network for trust estimation of unfamiliar users.

4.11 Communication module

The ZigBee based communication module makes use of the security services that are already present in the 802.15.4 security specification. ZigBee infrastructure security includes network access control, integrity of packet routing, and prevention of unauthorized use of packet transport. ZigBee application data security includes message integrity, authentication, freshness, and privacy(ZigBee Organization 2005).

5 Evaluations of the effect of collective wisdom on trust

The iTrust platform is designed to enhance the decision quality on trust evaluation via exploration of the proximal collective wisdom of the surrounding user groups. In the e-service environment, a multitude of transactions take place between anonymous sellers and buyers. Since users do not have permanent identities, they have to handle the trust problem. Mostly, a seller deals with this problem by insisting on payment in advance, thereby, protecting himself from deceitful buyers. The seller delivers the service package only after receiving payment from the buyer. The buyer therefore must be confident of the seller's willingness to deliver the service package.

Because the available e-service provision is highly dependent on the resources of the service provider, customers may not always get what they ask for. Aggressive sellers who are not able to provide requested services may decide to promote alternative choices, but customers may not want to

waste their computational resources on annoying spam messages. After receiving the seller's response, buyers have to decide whether to accept the provided choice. The interaction between the buyer and the seller can be formalized as a trust game discussed in several studies (Bolton et al. 2004; Buskens and Raub 2002; Coleman 1990; Dasgupta 2000) but we emphasize encouraging collaboration instead of the individual gain payoff (Fig. 3).

First, the buyer decides whether to accept the provided service and trust the seller. If buyer does not accept the alternatives or the buyer decides not to trust the seller, the interaction terminates and both parties forego the opportunity. If the buyer decides to trust the seller, a transaction takes place. In this transaction, the buyer transfers a valuable commodity to the seller (e.g. money). Then the seller decides whether to honor the trust shown by the buyer and to repay it with a commodity of equivalent value (e.g. e-service package) or to betray the buyer's trust and keep the money. If the seller decides to honor the trust shown by the buyer, both parties receive positive reputation reward. If the seller cheats the buyer, the seller receives the negative reputation as the punishment. In the special case that the user receive an alternative choice, some users will treat it as an annoying spam message while others may accept it and take it under consideration. In such a case, the reputation feedback is based on the decision of the user's behavior model.

Due to the asymmetric information, a customer does not have complete information about a seller's past behaviors. The only open accessible information is their global reputation. However, in a dynamic environment, where the user is in a distributed ad-hoc network environment, the available global reputation data are not able to satisfy user's need to make a quality decision. Customers must make use of the service provider's global reputation as well as the collective wisdom in their purchase decision. In the following sub-sections, several simulation experiments will be deployed to justify the performance of iTrust in the quality trust estimation. In section 5.1, the overall trust evaluation of iTrust will be verified to distinguish the performance of creditability investigation. In section 5.2, we will examine the effects using a dynamic environmental construct which includes the group size, ratio of buyers and sellers, the availability of information sources, as well as the proportion of user behavior scenarios. In section 5.3, the balance between iTrust interaction costs as well as the decision quality will be evaluated, which provides the reference material to determine the scope of future service applications.

5.1 Simulation design

In this simulation scenario, the goal is to verify whether the collective wisdom gathered from ubiquitous environment could improve the decision quality for estimating the trustworthiness of unfamiliar user. Two different reputation mechanisms are available for trust estimation: the traditional reputation mechanism allows users to estimate from the global reputation data and his/her owned personal transaction experience; the iTrust e-service equipped with credibility investigation module that can explore the collective wisdom of the ubiquitous environment as well as the global reputation data, and the user's personal experience.

In the ubiquitous environment, user's perishability and their anxiety level may strongly affect their interaction behaviors. User behaviors can be distinguished from the two dimensions and sorted into four stereotypes (Fig. 4). Perishability represents the level of urgency the user brings to completion of the task, the desire to obtain the service as soon as possible. With higher perishability, users prefer to

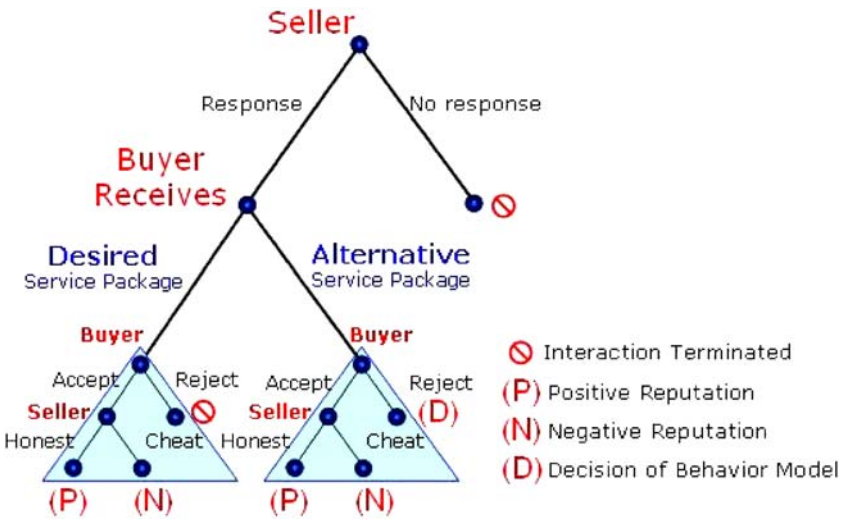


Fig. 3 Simple trust game scenario for evaluations

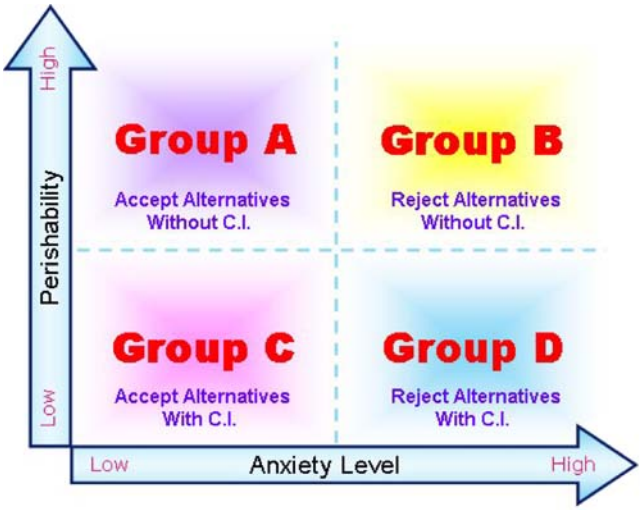


Fig. 4 User behavior stereotypes in the ubiquitous environment

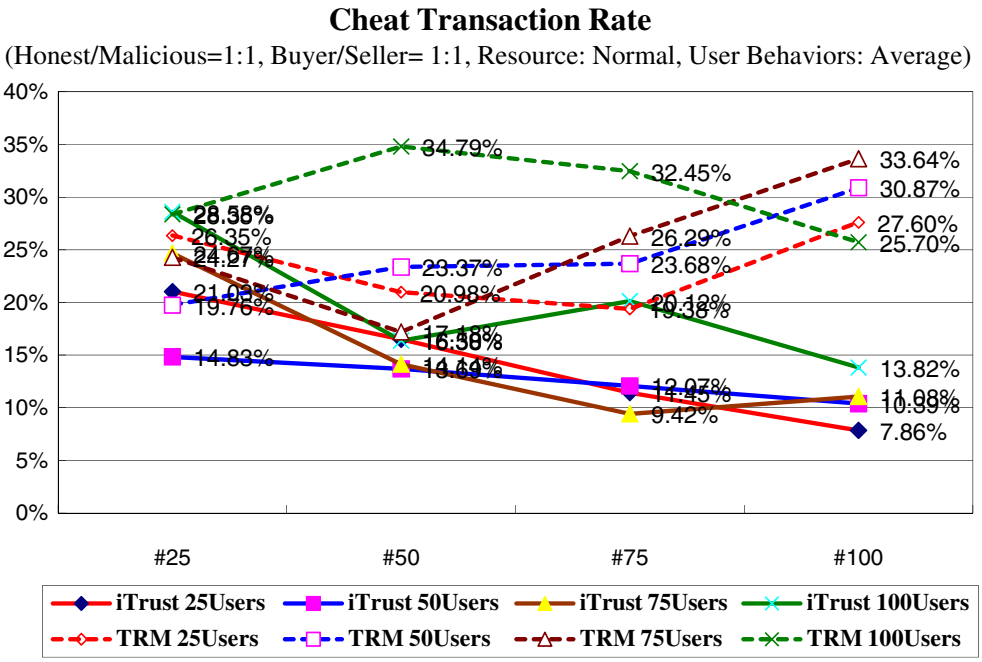
consume their resources (eq. time and processing capability, etc.) in service discovery rather than comparing which user is more reliable. Instead, once the service provision is acceptable and the provider's reliability fulfills their basic trustworthiness threshold, a transaction begins. The anxiety level represents the user's mental perception of security protection and how they view the probability of privacy intrusions and security breaches. Users with lower anxiety levels may consider various received service information as an alternative choice even though the provided services may not be related to their request. By contras, users with a high anxiety level are serious about whether the provider cares about their needs. Since accepting messages consumes a user's limited resources, spam messages or irrelevant service messages will be considered inimical actions.

The simulation experiment result is shown as the following diagrams: Fig. 5 represents the transaction cheat rate in the iTrust design and a traditional trust mechanism (TRM) design (e.g., e-Bay's). For the overall performance, we can see that iTrust improves the trust estimation of unfamiliar users and reduces the rate of transactions involving cheating to 15.83% in a risky environment that contains 50% cheaters, while TRM designs can reduce the average cheat transaction rate to 25.92%.

In the ad-hoc ubiquitous e-service environment there is rare information available for users to estimate which user is trustworthy. This problem is more serious when a new market is opened since the global reputation of each identity is zero and may not satisfy the user's trustworthiness threshold. This will lead to a desolate e-service environment since users may be afraid to transact with unfamiliar users. As the number of transactions increases, more interaction experience is stored in the environment. At the beginning stage the average cheat rate of iTrust is 22.28% while the TRM is 24.68%. After 100 transactions take place, the average cheat rate of iTrust falls to 10.79% while the TRM remains high at 29.45%. We can see that the cheat transaction rate of the iTrust decreases significantly when the number of transactions increases. But the cheat rate of the TRM design is remains at the initial levels.

For different group sizes in the e-service environment, small populations have a lower cheat transaction rate than big populations. Since in an unfamiliar environment, the smaller the group size, the easier it is for the user to

Fig. 5 Cheat Transaction Rate in iTrust and TRM designs



collaborate with the surrounding users to identify which user has an unusual potential risk. When in the bigger group, there are no rich interaction experiences available for users to estimate a specific user's trustworthiness.

In an ad-hoc e-service environment, people will be more careful to trade with those unfamiliar participants. Lake of trust or reliable information usually cause cautious users withdraw transactions. Figure 6 represents the successful transaction rate in the iTrust and TRM designs. In the risky environment setting, the successful transaction rate shows a significant difference between iTrust design and TRM design. Since the iTrust is equipped with a creditability investigation module that can gather nearby user's interaction experiences as an alternative information source for trust estimation, this design will diminish user's sense of insecurity and encourage users to carry on their transactions when they feel insecure about or unfamiliar with the transaction target. The TRM, lacking a creditability investigation module, takes only the self-owned experience and global reputation into consideration. However, in the beginning stages, that information is not enough to encourage users to participant in and embracing their desired e-services. The average successful transaction rate of iTrust is 98.70% while the TRM is 62.60%. The barrier for users to enter the unfamiliar e-service environment can be overcome by exploring the collective wisdom of the ubiquitous environment.

Simulation experiment results indicate that the iTrust design can enhance the decision quality by exploring the collective wisdom of the ubiquitous environment. Advanced simulations are briefly introduced in the following subsections.

5.2 Simulation: Dynamic environmental construct

Advanced simulations for understanding the effects of iTrust in a dynamic environment construct will be deployed in the following experimental items. This simulation experiment focuses on modulating the iTrust parameters in order to find the optimal situation for iTrust. Previous simulation takes places in a balance e-service environment that contains 50% of buyer and 50% of seller and the user behavior is in averagely distribution. Various types of distributions of seller-to-buyer ratio and user behaviors will be examined in the future to analyze possible marketing strategies in different e-service environments.

5.3 Part I. Healthy environment vs. malicious environment:

Lack of trustworthy infrastructure within the ad-hoc mobile e-service environment, each peer basically needs to maintain all threats in the environment on its own. iTrust enables the collective wisdom from e-service participants and supports collaborative trust evaluation of nearby users. It should be expected that iTrust could integrate available resources within an e-service environment to prevent malicious events. In order to evaluate the performance of iTrust in various situations, we then set up three kinds of environments: Healthy Environment, Malicious Environment, and Neutral Environment. The "Healthy Environment" contains 80% honest users and 20% malicious users. On the contrast, the "Malicious Environment" contains 80% malicious users and 20% honest users. A "Neutral Environment" has half honest users and half malicious users as a benchmark for normal environment settings. We stabilize

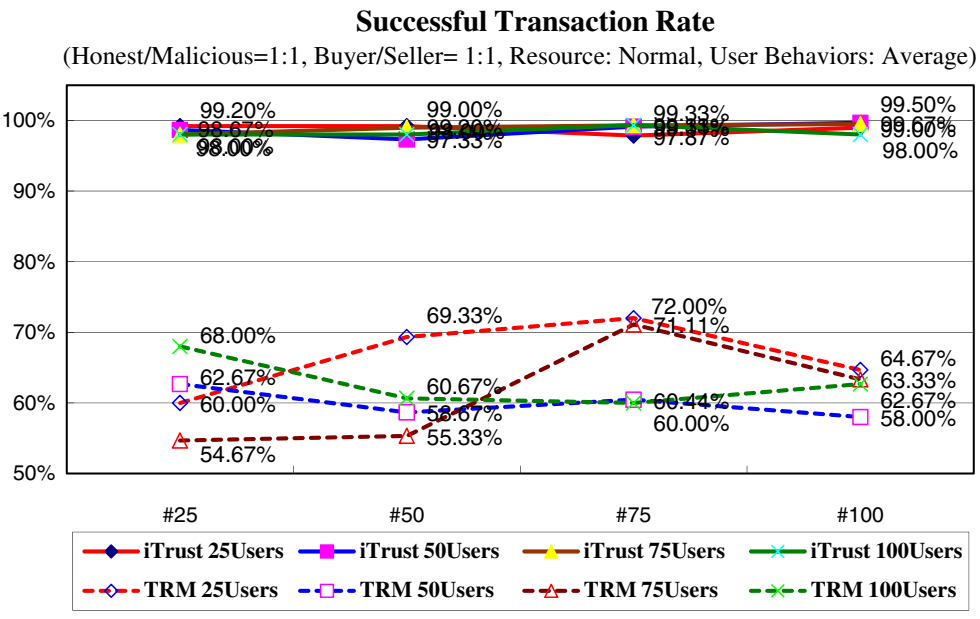


Fig. 6 Successful transaction rate in the iTrust and TRM designs

other parameter settings: there are 20 users within the e-service environment with a balanced buyer-to-seller ratio. User behaviors are assumed in normal distribution within a normal resource level.

Figure 7 illustrates that use of iTrust would help decrease cheat transaction rate. As interaction increases, the collective wisdom generated from participants' co-experience would assist deter cheat transactions. The use of iTrust is most effective in malicious environment—the cheat transaction rate could be lowered to 29% initially and would be down to 14% after 100 transactions take place. As in the "Healthy Environment", with the use of iTrust, cheat transaction rate would remain under 8% for the whole simulations and drop to 1% after 100 transactions take place. Simulation results indicate iTrust's collective wisdom mechanism would assist improve decision-making quality for all environment settings.

Figure 8 represents the successful transaction rates for iTrust in different environment settings. The average successful transaction rate of iTrust is above 98.8%. The iTrust encourages business transactions for all e-service participants. Meanwhile, the collective wisdom relies on experience sharing, and as a result the overall cheat transaction rate tends to decrease as more transactions take place within the e-service environment.

5.4 Part II. Buyer/ Seller ratio within e-Service environment:

Unbalanced market will affect supply and demand as well as success of transactions. A market which has more sellers than buyers gives buyers more opportunities for choosing desired trading partner, and so an ad-hoc unfamiliar e-service environment might enable buyers to find a relatively reliable trading partner more easily. In order to test the iTrust performance for different buyer-to-seller ratios within the e-service environment, the simulation was run under three kinds of setting modes. As usual, we stabilize any other parameters. The only difference among the setting modes is the buyer-to-seller ratio. The "More Buyer" environment contains 80% buyer and 20% seller while the "More Seller" environment contains 80% seller and 20% buyer. The "Neutral" environment uses equivalent buyer and seller as a benchmark for comparison with other two setting modes.

Figure 9 illustrates the cheat transaction rates in e-service environment with different buyer-to-seller ratios. Simulation shows unstable experiment results in cheat transaction rates for different buyer-to-seller ratio settings. The cheat transaction rates in both "More Buyer" and "More Seller" situations fluctuate all along the transactions. We found that as the desired service packages are sparse and held by malicious sellers, it tend to lead to a cheat transaction. Aside from these exceptional situations, iTrust could still help reduce the cheat transaction rate within the e-service environment. Therefore, advanced simulation regarding service provider's resource richness (i.e. substitutive ability) should be further examined.

Figure 10 represents the successful transaction rates for iTrust with different Buyer/Seller ratio settings. The average successful transaction rate of iTrust is above 96.9%. Again, iTrust encourages transactions successfully

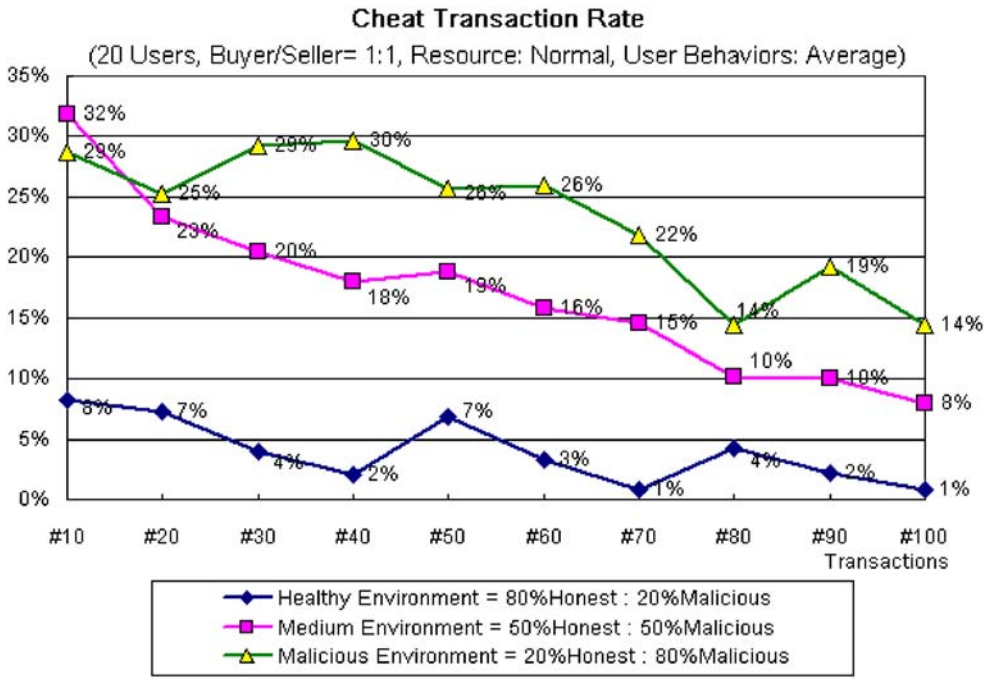


Fig. 7 Cheat transaction rate in Healthy/ Neutral /Malicious Environment

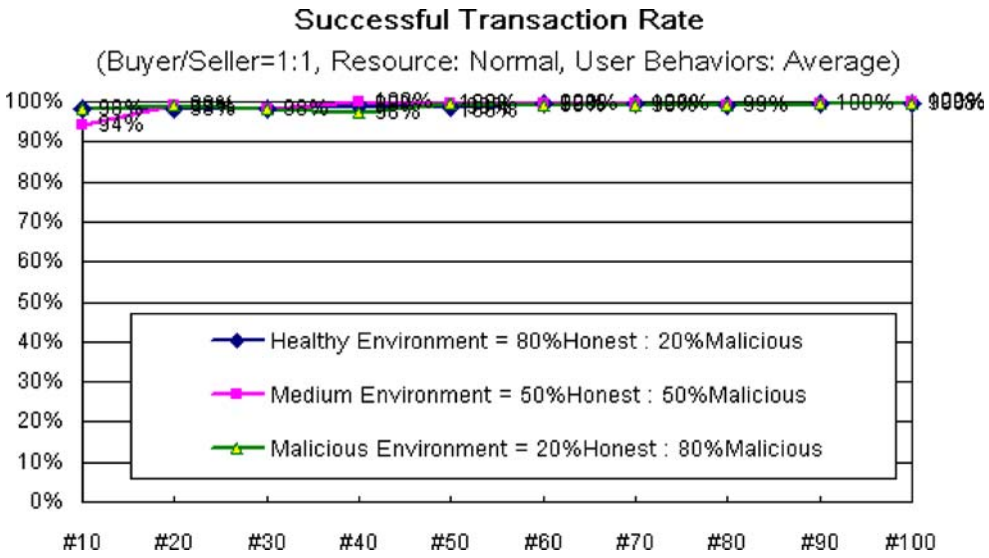


Fig. 8 Successful transaction rate in Healthy/Medium/ Malicious Environment

for all e-service participants. Capitalizing on more interaction experiences from the e-service environment, iTrust enables the overall cheat rate to decrease effectively.

5.5 Part III. Resource substitutive ability of service provider:

Seller's resource richness represents whether the seller can provide suitable service packages to the buyers. If some desired products are only held by malicious sellers, buyers then have no choice and must take risks. This experiment examines how different levels of resource substitutive ability will affect the successful transaction rate as well as the cheat transaction rate. There are two kinds of resource substitutive ability settings in the experimental environment. Rich resources substitutive ability represents different service providers may hold various similar service/products that may satisfy customer's needs. Buyers then have better chances to find replaceable service/products from other sellers. (i.e. Higher substitutive ability) On the contrast, poor resources substitutive ability represents that desired service/product are rare. Buyers can not find similar service/products from other service providers. Service providers then can monopolize some specific services which buyers are aspiring to obtain. We keep all other parameters unchanged in order to measure the effects of different resource substitutive abilities.

The simulation results are shown as Fig. 11. It is clear that the cheat transaction rate in high level substitutive ability situations decreases significantly. However, the cheat rate in low level substitutive ability is unstable (varies from 10% to 17%). In the poor substitutive ability situation,

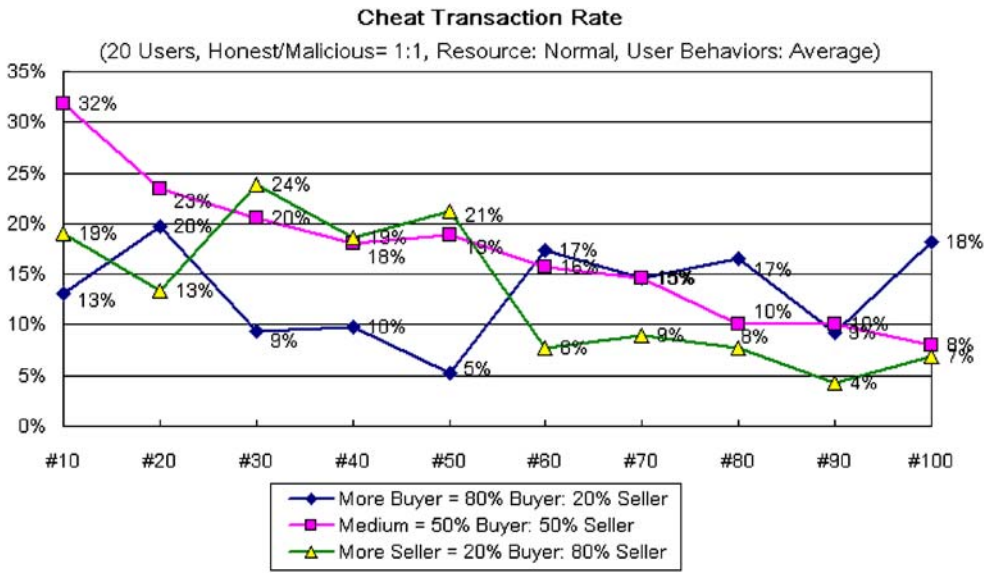


Fig. 9 Cheat transaction rate in different Buyer/Seller ratios

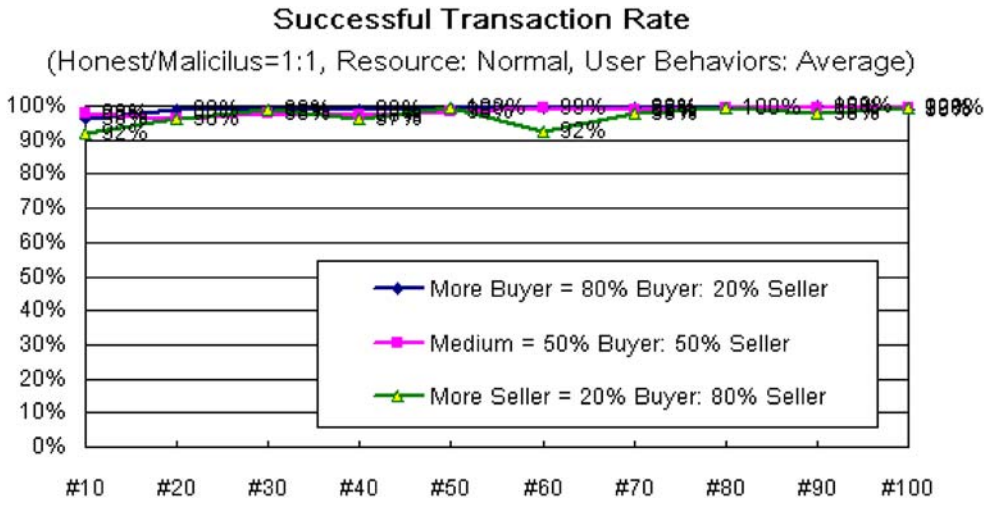


Fig. 10 Successful transaction rate in different Buyer/Seller ratios

once the desired service is only held by malicious users, cheat transaction is more likely to happen. Resources substitutive ability could affect cheat transaction rate. Poor resource substitutive ability might lead to exceptional problems if the resources were held by malicious service providers. In this specific situation, iTrust cannot do too much to prevent the malicious events.

5.6 Simulation: Interaction cost vs. decision quality

The following simulation experiment focuses on the system side. Heterogeneous information sources represent the possibility of bordering on the scope of collaborations. A larger number of transaction tasks taking place in the e-service environment may imply rich information availability, yet also higher interaction costs. The balance between interaction cost and decision quality should be examined to suggest the best e-service environment situation for the iTrust. Average system interaction cost would be analyzed against improved decision quality.

5.7 Large scale simulations:

The first part of the simulation experiment takes place with large group size for large scale transactions. Up to 3,000 transactions will be simulated within four different group sizes. Considering the environmental limitations that ZigBee supports short-range transmissions, the group size of participants in ubiquitous e-service environment are unfolded into four types—25 users, 50 users, 75 users and 100 users—for simulation experiments. The experiment is designed for exploring the feasible general environmental parameter settings regarding group size and transaction number that should be further observed.

Simulation experiment regarding iTrust performance in different group sizes and transaction settings are shown as Fig. 12. In a hazardous environment that contains 50% malicious users, we wish to lower the cheat transaction rate to below 10% with reasonable interactions. As the ad-hoc ubiquitous e-service highlights dynamic interactions and focuses on the value of the moment, long ago interaction

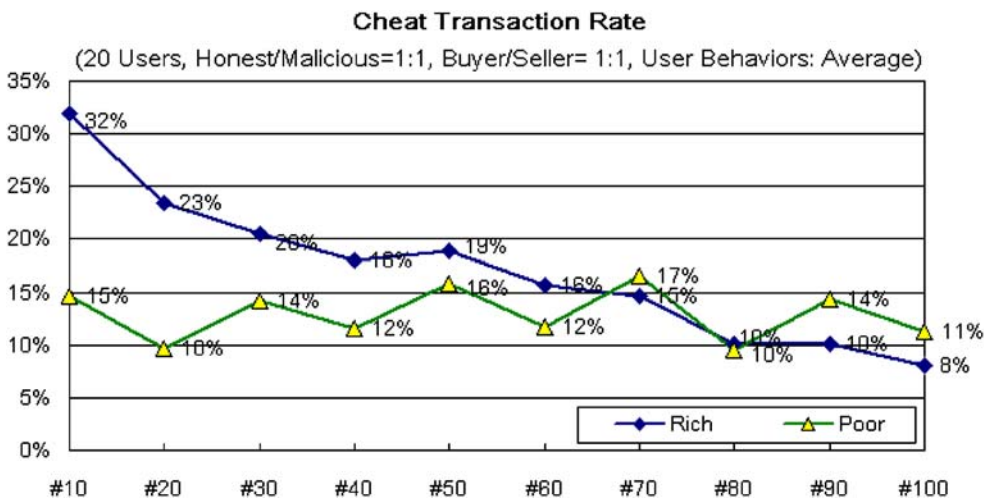
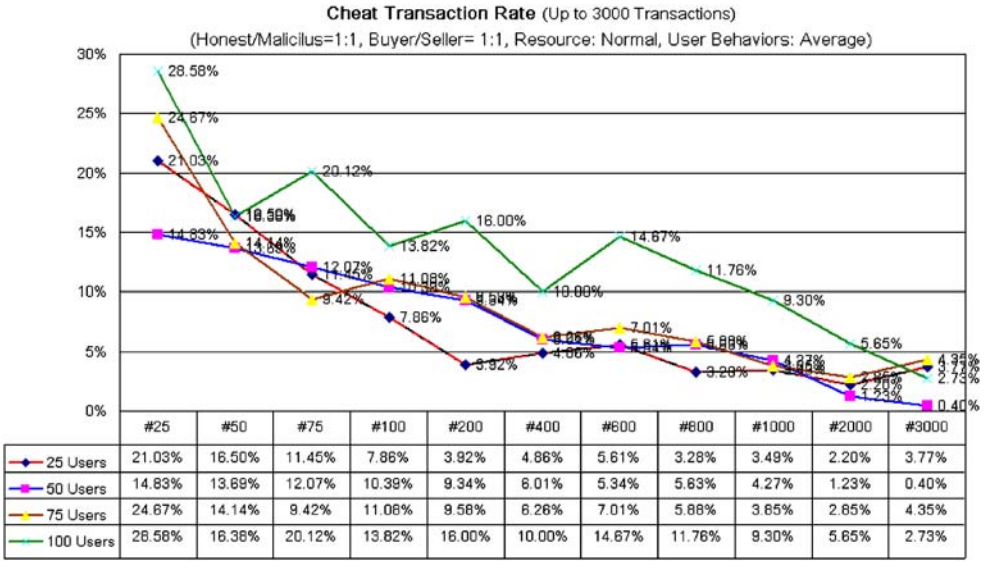


Fig. 11 Cheat transaction rate in different resource substitutive ability

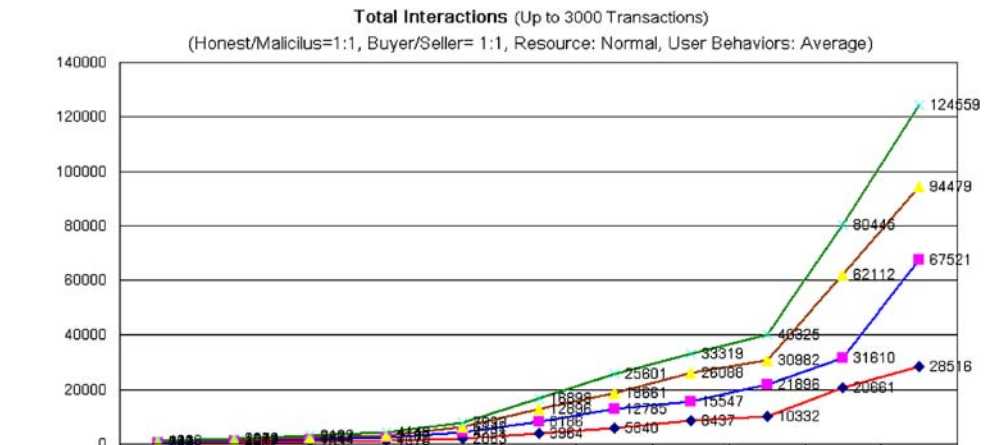


	#25	#50	#75	#100	#200	#400	#600	#800	#1000	#2000	#3000
25 Users	21.03%	16.50%	11.45%	7.86%	3.92%	4.86%	5.61%	3.28%	3.49%	2.20%	3.77%
50 Users	14.83%	13.69%	12.07%	10.39%	9.34%	6.01%	5.34%	5.63%	4.27%	1.23%	0.40%
75 Users	24.67%	14.14%	9.42%	11.08%	9.58%	6.26%	7.01%	5.88%	3.65%	2.65%	4.35%
100 Users	28.58%	16.36%	20.12%	13.82%	16.00%	10.00%	14.67%	11.76%	9.30%	5.65%	2.73%

experiences may be useless in improving the iTrust performance. Although the simulation result indicates the cheat rate for all parameter settings would be below 5% after 3,000 transactions. However, it is not reasonable to assume such extensive interactions may take place in a short period of time especially in such an ad-hoc e-service environment. Moreover, according to the communications shown in Fig. 13, the interaction costs are comparably high in such extensive interaction situations. It is more reasonable to assume that the distribution of e-service participants would be sparser rather than a crowded deployment. Based on aforementioned reasons, advanced experiments will focus on the group size less than 25 users and observe the iTrust performance under 100 transactions hereafter.

5.8 Small group simulations

Based on the simulations results, we suggest that the advanced simulation experiments should focus on small group interactions. The second part of the simulation experiment takes place with five smaller group sizes within a certain limited scale of transactions. The group sizes fall into five categories: 5 users, 10 users, 15 users, 20 users and 25 users within the e-service environments. The objectives of the simulation experiment are to verify the performance as well as to find acceptable interaction costs of iTrust in small group interactions. Both Malicious/Honest user ratio and the Buyer/Seller ratio are set to be equal, respectively. Also, the user behavior types are normally distributed. Resource richness is set in a neutral level. The performance of iTrust in the small



	#25	#50	#75	#100	#200	#400	#600	#800	#1000	#2000	#3000
25 Users	243	480	703	1070	2083	3964	5840	8437	10332	20661	28516
50 Users	514	1017	1514	2173	4201	8186	12785	15547	21896	31610	67521
75 Users	799	1594	2294	3187	6142	12896	18661	26088	30982	62112	94479
100 Users	1036	2079	3122	4146	7992	16898	25601	33319	40325	80445	124559

group experiments shows in the same manner as that in the large scale simulations. Collective wisdom of iTrust generated from user interactions assists reduce the cheat rate smoothly and keeps it under 10% after 50 transactions under all scenarios. Figure 14 clearly presents the performance of iTrust in the small group simulations.

Figure 15 represents the interaction costs for communication among e-service participants. Comparing with large scale simulations among large group size participants, the interactions costs among small group sizes are relatively affordable in a mobile environment. The more participants within the e-service environment, the more interactive communications must take place. As interactions increase, more experiences will be gained and shared within the e-service environment. The heterogeneous information sources are indispensable for quality decision-making, especially in the ad-hoc e-service environment.

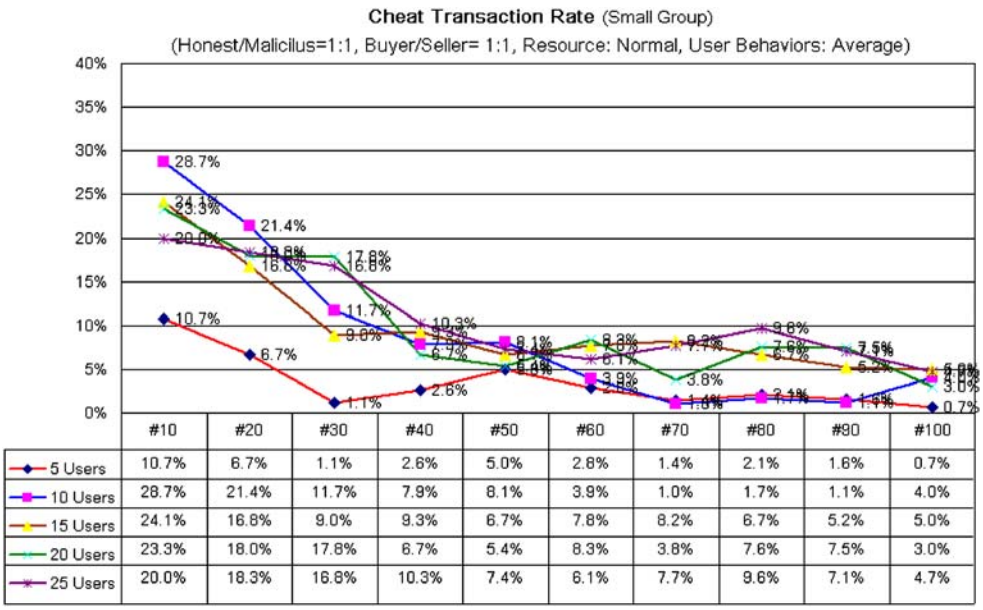
The results of successful transaction rate experiment are shown as Fig. 16, in which one may see the rate is more than 90% in the initial stage for most of the cases. iTrust could encourage unfamiliar e-service participants' collaboration and therefore to facilitate the transactions successfully.

The simulation results clearly show that iTrust e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. The iTrust e-service realizes the collective wisdom and provides a feasible solution for quality decisions in the dynamic and distributed environment.

5.9 Significance & contribution of the iTrust platform

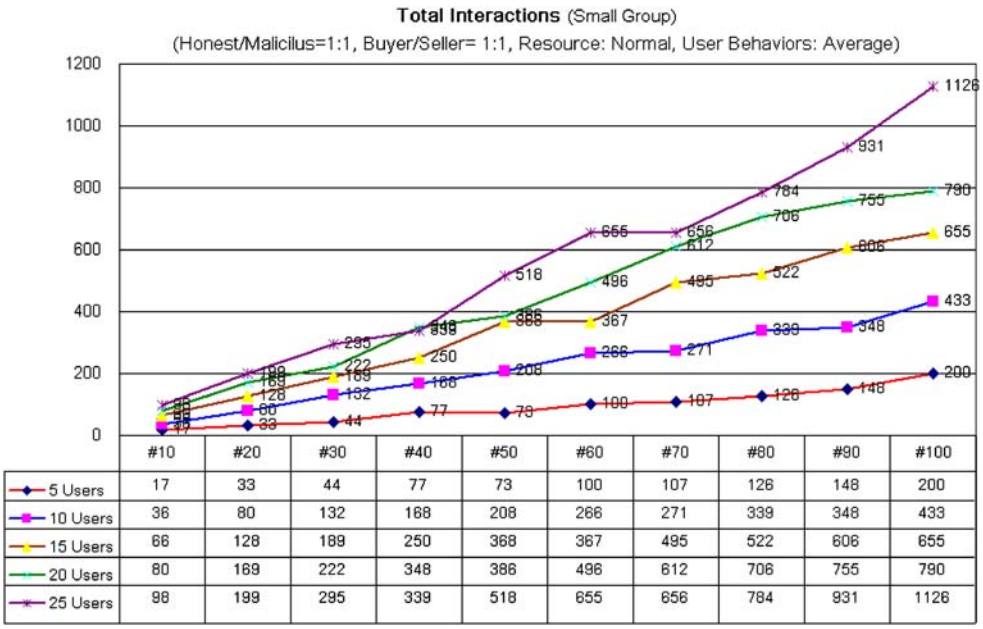
Considering the natural limitations of ad-hoc ubiquitous e-service environment, our iTrust design has several significant improvements and contributions. The collaborative iTrust platform accordingly is empowered to realize the vision of ubiquitous iTrust e-service in terms of the following perspectives:

- Deliberation of short-term lived pseudonyms:
  Revises existing long term identity design concepts and ensures the unlinkability of identities.
- Distributed data process consideration:
  Each interaction record within the iTrust e-service environment relies on the computational loading and data storage in the mobile device instead of the centralized server database.
- Lightweight consideration:
  Different from the existing works of centralized gradational pseudonym design (the quantity of interaction data will be expanded in exponential growth), our design method integrates a user's conceptual role information and relationship information into an abstract public information attached to the user's identity. This attached abstract information can then provide hints to filter out inadequate service information that will reduce unnecessary data transmission. Since the required feature of lightweight computation for mobile devices is emphasized, our design reduces considerable expansion and makes it adequate to the ubiquitous e-service. Moreover, the adoption of the time stamp design is exerted to omit those overdue historical interaction data, which will further improve the strength of interaction pseudonym's unlinkability.
- Convenience requirement:
  Under the versioning scheme, irrelevant service information is filtered out. Only highly correlated services are delivered to the requester. The versioning design reduces



	#10	#20	#30	#40	#50	#60	#70	#80	#90	#100
5 Users	10.7%	6.7%	1.1%	2.6%	5.0%	2.8%	1.4%	2.1%	1.6%	0.7%
10 Users	28.7%	21.4%	11.7%	7.9%	8.1%	3.9%	1.0%	1.7%	1.1%	4.0%
15 Users	24.1%	16.8%	9.0%	9.3%	6.7%	7.8%	8.2%	6.7%	5.2%	5.0%
20 Users	23.3%	18.0%	17.8%	6.7%	5.4%	8.3%	3.8%	7.6%	7.5%	3.0%
25 Users	20.0%	18.3%	16.8%	10.3%	7.4%	6.1%	7.7%	9.6%	7.1%	4.7%

Fig. 14 Cheat transaction rate for applying iTrust in small groups



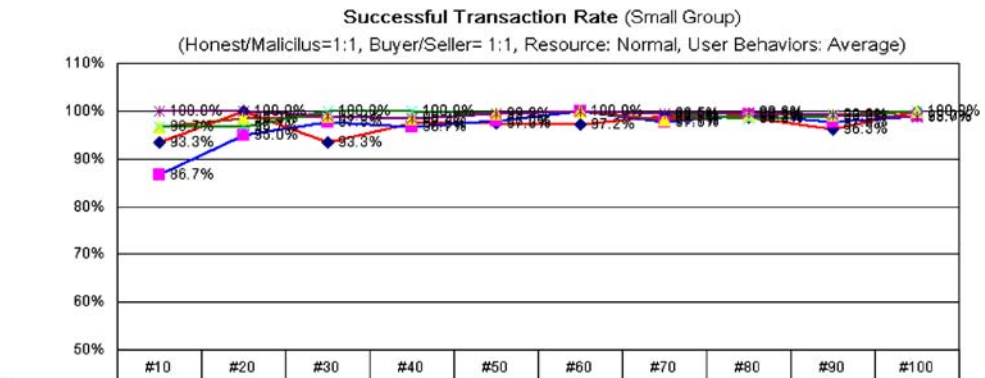
	#10	#20	#30	#40	#50	#60	#70	#80	#90	#100
5 Users	17	33	44	77	73	100	107	126	148	200
10 Users	36	80	132	168	208	266	271	339	348	433
15 Users	66	128	189	250	368	367	495	522	606	655
20 Users	80	169	222	348	386	496	612	706	755	790
25 Users	98	199	295	339	518	655	656	784	931	1126

Fig. 15 The interaction cost for applying iTrust in small groups

communication costs and system loading while improving service efficiency.

5.10 Related works

Due to the storage and communicational limitation of mobile devices in an ad-hoc e-service environment, not all the trust data could be retrieved wherever needed or stored in the mobile devices. Most of related studies are focused on the fixed Internet environment (Aberer and Despotovic 2001; Enzmann and Schneider 2004; Enzmann and Schneider 2005; Golbeck et al. 2003; Kinateder and Rothermel 2003; Lin et al. 2004; Sabater and Sierra 2002), where the trustworthy information are always available. Little is known about the ad-hoc ubiquitous environment or wireless distributed network environments (Lin et al. 2004; Shand et al. 2004; Wilhelm et al. 2000). Naturally comes to a question—"How the trustworthiness is computed in the ad-hoc ubiquitous environment"? There are two approaches about how to acquire available trust data. The local computation design calculates the trust data only from the locally obtained data (Aberer and Despotovic 2001; Gupta et al. 2003; Shand et al. 2004; Twigg 2003), while the global trust computation calculates from the entire trust data stored in disparate sources (Aberer and Despotovic 2001; Castelfranchi et al. 2003; Lin et al. 2004; Mui et al. 2003; Sabater and Sierra 2002). Based on the concept of proximity collective wisdom, users may also compute one's trustworthiness from the other proximal persons that they trust. In our study, we integrate all available information



	#10	#20	#30	#40	#50	#60	#70	#80	#90	#100
5 Users	93.3%	100.0%	93.3%	97.5%	97.3%	97.2%	99.0%	98.8%	96.3%	100.0%
10 Users	86.7%	95.0%	97.8%	96.7%	98.0%	100.0%	97.6%	99.2%	97.8%	99.0%
15 Users	96.7%	98.3%	98.9%	98.3%	99.3%	100.0%	98.1%	99.2%	99.3%	100.0%
20 Users	96.7%	96.7%	100.0%	100.0%	99.3%	100.0%	99.5%	98.3%	98.9%	100.0%
25 Users	100.0%	100.0%	98.9%	98.3%	99.3%	100.0%	99.5%	99.6%	99.3%	98.7%

Fig. 16 Successful transaction rate for small group simulations

sources in the ad-hoc ubiquitous environment and using collaborative content-based filtering to compute trust without direct experience.

An ad-hoc ubiquitous environment relies on all participants actively contributing to network activities. Existing studies are facing the problems of information availability and trust data updating in the ad-hoc ubiquitous environment. For example, Lin proposed a distributed trust management broker framework for e-services, but in their framework each user is associated with a broker that collects the trust ratings of all its service providers for its users. Namely, the reputation authority was designed as a universal database that collects trust information from brokers and stores trust information for all the users. However, this universal database would not be updated frequently, and its performance relies on the broker network's reliability. In the other work, Shand et al proposed a trust and risk framework to facilitate secure collaboration in ubiquitous computer systems. However, their works also assume the availability of updated and relevant information sources that could be guaranteed through their trusted network.

Due to the dynamic changes of environment, available information sources are seldom available in the ad-hoc ubiquitous environment. By highlighting the homophily of e-service participants, social network support enables mobile users to collaborate with proximity groups for contributing the collective wisdom. Our proposed iTrust platform is a design that is believed to support the needs and nature characteristics of the ad-hoc e-service environment.

6 Conclusion

Trust has been considered as a top criterion for the acceptance of e-service adoption. This paper presents a ubiquitous iTrust platform that exerts the identity design to deliver the visions of ubiquitous collaborative trustworthy e-service with an integrated consideration of trust, reputation and privacy requirements. It is proposed to provide a feasible solution for quality decisions in the dynamic and distributed ubiquitous environment. By highlighting the homophily of e-service participants, these isolated individuals can be treated as a group with proximity. Proximity thus enables ad-hoc e-service participants to contribute their strength for ubiquitous collective wisdom. We proposed the notion of iTrust e-Service which highlights the collective effort focused on collecting the user group's power as the reference for ubiquitous trust decisions. We have implemented the iTrust platform and evaluated the design and the platform from different perspectives (trust, reputation, privacy, efficiency, usability, etc.). Simulation evaluations results indicate the iTrust design can eliminate potential risk and provide appropriate estimation for trust decision in the ad-hoc ubiquitous environment. As homophylic user groups are more likely to combine the strength of different individuals to achieve specific objectives. The ubiquitous proximity e-service makes it possible for users to collaborate with the proximity user groups for establishing a reliable and trustworthy interaction environment. The future fruitful research includes the application of the iTrust design to various kinds of homophily identified among proximal e-service participants.

References

Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. CIKM'01, 310–317.

Allen, T. J. (1977). *Managing the flow of technology*. Cambridge, MA: MIT.

Anderson, B. (1983). *Imagined communities*. London: Verso.

Aristotle, & Rackham, H., translator. (1934). *The nicomachean ethics*. Cambridge, MA: Harvard University Press.

Bolton, G. E., Katok, E., & Ockenfels, A. (2004). Trust among internet traders: a behavioral economics approach. *Analyse und Kritik*, *26*, 185–202.

Buskens, V., & Raub, W. (2002). Embedded trust: Control and learning. *Group Cohesion, Trust and Solidarity*, *19*, 167–202.

Castelfranchi, C., Falcone, R., & Pezzulo, G. (2003). Integrating trustfulness and decision using fuzzy cognitive maps. Trust Management 2003, LNCS 2692, 195–210.

Coleman, J. S. (1990). *Foundations of social theory*. Cambridge, MA: The Belknap Press of Harvard University Press.

Dasgupta, P. (2000). Trust as a commodity. In D. Gambetta (Eds.), *Trust: Making and Breaking Cooperative Relations, electronic edition*. University of Oxford: Department of Sociology http://www.sociology.ox.ac.uk/papers/dasgupta49-72.pdf.

Earle, T. C., & Cvetkovich, G. T. (1995). *Social trust: Towards A cosmopolitan society*. Praeger Publishers: Westport, CT.

Enzmann, M., & Schneider, M. (2004). A privacy-friendly loyalty system for electronic marketplaces. Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE04), Taiwan.

Enzmann, M., & Schneider, M. (2005). Improving customer retention in E-commerce through a secure and privacy-enhanced loyalty system. forthcoming: Information Systems Frontiers.

Festinger, L., Schachter, S., & Back, S. (1950). *Social pressures in informal groups: A study of human factors in housing*. Palo Alto, CA: Stanford University Press.

Golbeck, J., Parsia, B., & Hendler, J. (2003). Trust networks on the semantic web. Proceedings of Cooperative Intelligent Agents 2003.

Govier, T. (1997). *Social trust and human communities*. McGill-Queen's University Press.

Gupta, M., Judge, P., & Ammar, M. (2003). A reputation system for peer-to-peer networks. NOSSDAV'03, 144–152.

Habermas, J. (1991). *The structural transformation of the public sphere*. Cambridge, MA: MIT Press.

Hwang, Y. C., & Yuan, S. T. (2007). A privacy-aware identity design for exploring ubiquitous collaborative wisdom. *Lecture Notes in Computer Science (LNCS)*, *4490*, 433–440.

Kinateder, M., & Rothermel, K. (2003). Architecture and algorithms for a distributed reputation system. Trust Management 2003, LNCS 2692, 1–16.

Lazarsfeld, P., & Merton, R. K. (1954). *Friendship as a social process: A substantive and methodological analysis, freedom and control in modern society*. New York: Van Nostrand.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, *63*, 967–985.

Lin, K., Lu, H., & Yu, T. (2004). A distributed trust and reputation management framework for E-services. IEEE International Conference on Services Computing.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpe. *Academy of Management Journal*, *38*(1), 24–59.

McKnight, D., & Chervany, N. (2002). What trust means in E-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, *6*(2), 33–59, 2001.

Mui, L., Halberstadt, A., & Mohtashemi, M. (2003). Evaluating reputation in multi-agents systems. AAMAS2002 Ws Trust, Reputation. LNAI 2631, 123–137.

Plato. (1968). *Laws. Plato in twelve volumes, vol. 11*. Cambridge: Harvard University Press.

Sabater, J., & Sierra, C. (2002). Reputation and social network analysis in multi-agent systems. AAMAS'02, 475–482.

Shand, B., Dimmock, N., & Bacon, J. (2004). Trust for Ubiquitous, Transparent Collaboration. *Wireless Networks*, *10*(6), 711–721.

Singh, J., & Sirdeshmukh, D. (2000). Agency and trust mechanisms in consumer satisfaction and loyalty judgments. *Academy of Marketing Science*, *28*(1), 150–167.

Twigg, A. (2003). A subjective approach to routing in P2P and ad hoc networks. Trust Management 2003, LNCS 2692, 225–238.

Weiser, M. (1991). The computer of the 21st century. *Scientific American*, *265*(3), 66–75.

Wilhelm, U. G., Staamann, S. M., & Buttyan, L. (2000). A pesimistic approach to trust in mobile agent platforms. *IEEE Internet Computing*, 40–48.

ZigBee Organization (2005). ZigBee specification ver. 1.0, http://www.zigbee.org

Yuan-Chu Hwang received his Ph.D. from MIS Department of National Chengchi University in 2007. Currently, he is an Assistant Professor of Information Management Department in National United University in Taiwan. Dr. Hwang's research and teaching interests include e-service innovation, ubiquitous commerce and privacy/trust issues for social mobile applications.

Soe-Tsyr Yuan received her Ph.D from Computer Science Department of Oregon State University in USA. Currently, she is a Professor of Information Management in College of Commerce of National Chengchi University in Taiwan. Her contemporary research areas include mobile/ubiquitous commerce, intelligent agents and data mining, service-oriented computing and Service Science.