Winter 12-2-2007

U-ATM: An Autonomous Trust Model for Exploring Ubiquitous Collective

Yuan-Chu Hwang

Proceedings of The Seventh International Conference on Electronic Business, Taipei, Taiwan, December 2-6, 2007, pp. 96-101.

U-ATM: AN AUTONOMOUS TRUST MODEL FOR EXPLORING UBIQUITOUS COLLECTIVE WISDOM

Yuan-Chu Hwang, National United University, Taiwan, ychwang@nuu.edu.tw

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 user to embracing these ubiquitous e-services, we propose an Autonomous Trust Model for exploring collective wisdom in the ubiquitous environment (hereafter termed "U-ATM") as an instance of ASEM. ASEM (Ambient e-Service Embracing Model) addresses the core elements (of relevance to the integrated concern of trust, reputation and privacy) required for assuring such desired features as convenience, safety, fairness and collaboration for mobile users when they engage with ambient e-services. The U-ATM highlights the distributed peer-to-peer interactions under an ad-hoc network composition. It especially accommodates the dynamic short-lived identity characteristics and lightweight computational capacity of mobile devices. The U-ATM we have developed is based on the ZigBee architecture as a collaborative application in the upper layer of the ubiquitous environment. U-ATM design concepts are elaborated and evaluated. A simulation is conducted. Simulation outcomes for trust decision quality enhancement show significant improvement over traditional designs. U-ATM 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.

CHALLENGES FOR UBIQUITOUS E-SERVICE

The ongoing, rapid developments in information systems technologies and networking have 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. Unfortunately, such a rapid technological evolution cannot be problem free. Concerns are raised regarding the 'lack of trust' in ubiquitous e-service environment and 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 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. The notion of ambient e-services is proposed to identify a new scope of ubiquitous e-service, which addresses dynamic collective efforts between mobile users (enabled by Mobile-P2P technology), dynamic interactions with ambient environments (envisioned by Location-Based Services), moment of value, and low cost service provision. 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 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.

To solve the problem of creating trust in the ubiquitous environment, we propose an collaborative trust e-service for exploring the collective wisdom in the ubiquitous environment, called "U-ATM". The U-ATM e-service is an ambient e-service application that may obtain value-added information through the interactions of surrounding environments and/or users. The U-ATM e-service allows users to choose and cooperate with trustworthy partners for executing transactions in the risky ubiquitous environment. The U-ATM 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 U-ATM e-Service highlights the collective effort focused on collecting the user group's power as the reference for ubiquitous trust decisions.

THE COLLABORATIVE STRENGTH OF U-ATM 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 ambient e-Service was 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 U-ATM 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, 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?

Exploring Proximal Intelligence: Experience Co-Creation

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 U-ATM 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 seldom information available for trust decision in an ad-hoc ubiquitous environment. The U-ATM e-service extends the information sources from traditional commerce scenarios that consider the transaction-based experience only. Instead, interaction-based experiences are also 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. 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? 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.

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 U-ATM e-Service, a creditability investigation module is designed for experience sharing collaboration. Detailed descriptions of U-ATM components are illustrated in the Section 3.2. After the creditability investigation process is completed, users may have 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 creditability 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 creditability 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 U-ATM 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 interaction-based experience from self-owned interaction pseudonyms. WNLT represents the weight of interpersonal interaction-based experience from creditability investigation. WGR represents the weight of transaction-based global reputation. The final score computation for trust candidate selection is shown as formula (1).

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

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.

U-ATM E-SERVICE DESIGN

We have identified the major challenges in an ubiquitous environment and the urgent needs for collaborative U-ATM e-service. We use an U-ATM 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 U-ATM 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 U-ATM 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.

U-ATM Privacy and Security Design

The U-ATM privacy design concept is based on multiple layered pseudonyms to ensure identity security and unlinkability. The U-ATM 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 abstract 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, U-ATM design uses a transaction pseudonym to ensure safety for a onetime 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 (Figure 1A) 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 cannot change their active pseudonym without cost. Detailed security design and evaluations can be found in [2].

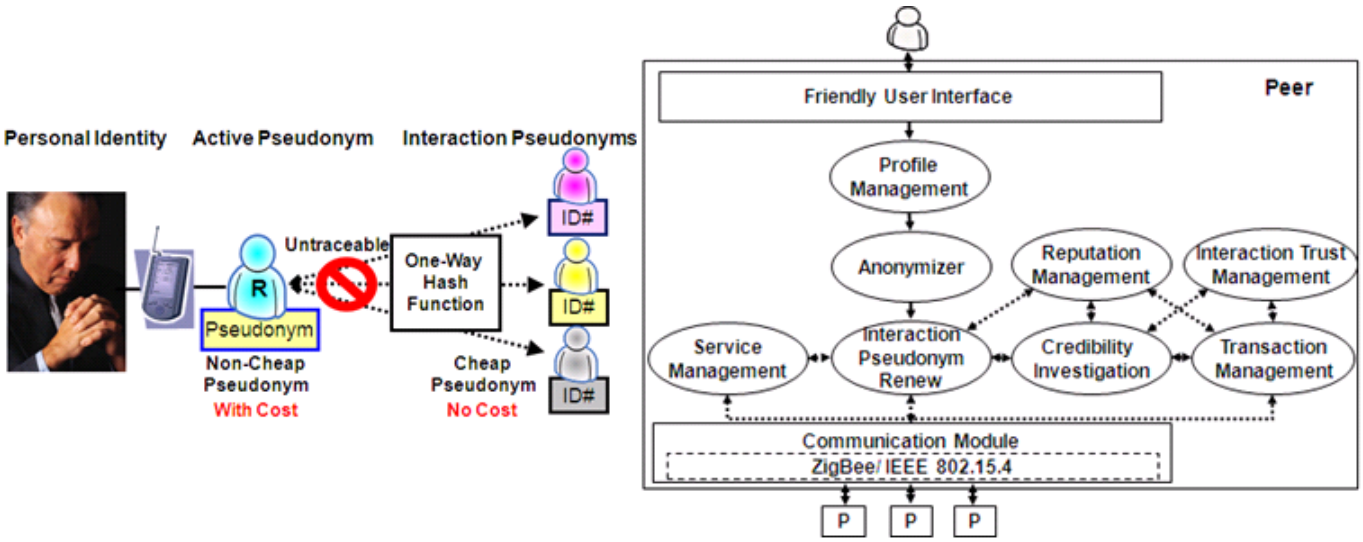

FIGURE 1. (A) General idea and relationships between the pseudonyms (B) Macro view of the Collaborative U-ATM platform

U-ATM Platform Design

The U-ATM e-service platform as well as it's function modules are depicted in Figure 1B. Including:

Profile Management

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

Anonymizer

In the U-ATM 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.

Interaction Pseudonym Renew

As mentioned in previous sections, U-ATM 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 creditability investigation, is targeted to those identities obtained by Interaction Pseudonym Renew module.

Service Management

Service management in the U-ATM 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 Creditability Investigation module for advanced decision-making.

Creditability 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 U-ATM e-service platform, the traditional transaction-based experience is considered for decision-making, along with the interaction-based experiences. For creditability 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 U-ATM 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 Creditability Investigation module filters out credible candidates for further transaction management.

Transaction Management

After the user has determined the target peer for transaction, a transaction pseudonym is created automatically in the U-ATM 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.

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 creditability investigation, but is also linked to the Interaction Pseudonym renew module for global reputation updates.

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 Creditability Investigation module, it provides heterogeneous information based on user experiences stored in the social network for trust estimation of unfamiliar users.

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.

EFFECT OF COLLECTIVE WISDOM

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 U-ATM 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 4 stereotypes. 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 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 contrast, 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.

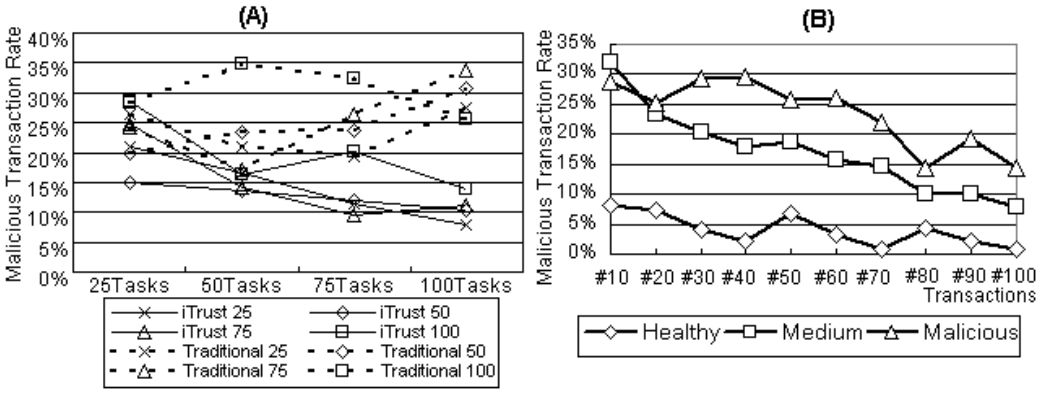

FIGURE 2. (A) Cheat Transaction Rate in U-ATM e-service and Traditional designs
(B) Cheat Transaction Rate in Healthy/Malicious environment

The simulation experiment result is shown as the following diagrams: Figure 2A represents the transaction cheat rate in the U-ATM e-service and Traditional designs. Up to 100 transactions were executed by users with different group size. In testing the performance of collaborative trust, we have considered practical factors such as the population of malicious hosts and good hosts; the available peer numbers to simulate realistic conditions for real applications. For the overall performance, we can see that U-ATM 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 Traditional designs can reduce the average cheat transaction rate to 25.92%. In the ubiquitous e-service environment it is lack of 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 U-ATM is 22.28% while the Traditional is 24.68%. After 100 transactions, the average cheat rate of U-ATM falls to 10.79% while the Traditional remains high at 29.45%. We can see that the cheat transaction rate of U-ATM decreases significantly when the number of transactions increases. But the cheat rate of the traditional design still remains at the initial levels.

To evaluate the performance of U-ATM collective wisdom, different kinds of environments have been established which contains varied proportion of users. The healthy environment contains 80% honest users and 20% cheaters. On the contrary, the malicious environment contains 80% cheaters and 20% honest users. Figure 2B represents the power of collective wisdom in various environments. The experience co-creation approach could retrieve heterogeneous information sources to help users identify malicious node and prevent cheating. In the malicious environment, even in the initial stage, U-ATM reduces the rate of transactions involving cheating to 28.67% in an extremely risky environment that contains 80% cheaters. After 100 interactions, the malicious transaction rate could be decreased to a level below 15% for all kinds of environments. The simulation results clearly show that U-ATM e-service makes it possible for users to collaborate with the nearby user groups for establishing a reliable and trustworthy interaction environment. The U-ATM e-service realizes the collective wisdom and provides a feasible solution for quality decisions in the dynamic and distributed environment.

SIGNIFICANCE & CONTRIBUTION CONCLUSIONS

Trust has been considered as a top criterion for the acceptance of e-service adoption. This paper proposes a ubiquitous U-ATM platform that exerts the identity design to deliver the visions of collaborative trust e-service with an integrated consideration of trust, reputation and privacy requirements. Different from traditional architecture, the U-ATM highlights the distributed peer-to-peer interaction under ad-hoc network composition, especially to accommodate the dynamic short-lived identity characteristics and the lightweight computational capacities of mobile devices. We deploy our U-ATM based on the ZigBee architecture as an upper layered collaborative application in the ubiquitous environment. The U-ATM design concepts are elaborated and evaluated. U-ATM simulation outcomes for trust decision quality enhancement are significantly improved by comparison with traditional designs. The simulation experiments illustrate the benefits of exploring the collective wisdom and gathering the power of collaboration. Moreover, the U-ATM makes it possible to collaborate with nearby user groups for establishing reliable and trustworthy interaction environments. It also facilitates and empowers the potential benefits for various ubiquitous e-service applications. Possible future research includes field experiment for applying U-ATM in different business scenarios. Ubiquitous i-Network that enables users exploring the collective wisdom for rich collaboration rather than just information diffusion in proximity e-service environments is also worthy of further in-depth research.

REFERENCES

[1] Hwang, Y. C. and Yuan S.T. (2007) "A Roadmap for Ambient E-Service: Applications and Embracing Model", *International Journal of E-Business Research*, Vol. 3, No. 1, pp. 51-73.

[2] Hwang, Y. C. and Yuan S.T. (2007) "A Privacy-Aware Identity Design for Exploring Ubiquitous Collaborative Wisdom", *Lecture Notes in Computer Science (LNCS)*, Vol. 4490, pp. 433-440.