A Fuzzy Trust Evaluation Model in Mobile Commerce

J. Chen, Z.Y. Cai
College of Computer and Information technology
China Three Gorges University
Yichang, China

J. Peng
College of Civil Engineering & Architecture
China Three Gorges University
Yichang, China

***Abstract*—With the quick development of mobile commerce, lacking of trust and security is becoming a big obstacle to the development of the mobile commerce. In this paper, the reliability and security problem of mobile commerce, especially trust evaluation model in its operation are studied, and a trust evaluation model based on fuzzy mathematics is proposed. Then in order to gain a comprehensive trust value of the whole mobile commerce, the fuzzy recommend and combined algorithm is presented. Lastly the proposed model is verified by an example.**

Keywords-mobile commerce; information security; trust evaluation; fuzzy mathematics

I. INTRODUCTION

Since there are great uncertainty and subjective factors in mobile commerce, many early researches have focused on mobile payment trust. Their results have shown that from the point of view of the original trust, the impact of two factors affected the performance and willingness of users [1,5,6]. Trust benefits people who live in a risky and uncertain situation by providing means to decrease complexity. Trust is the key to decision making; thus visualizing trust information could benefit users' behavior and decisions [2]. On one hand, trust research provides empirical evidences to illustrate the coexistence of integrity trust and distrust. Generally, if an individual trusts the integrity of a service provider, the cause is more likely to keep its promise of providing genuine personalized mobile services by a substantial investment in location detection technologies. On the other hand, if the individual distrusts the integrity of a service provider, it is the subsequence of this investment that the service provider has a strong incentive to cheat others in order to justify the investment [3,4].

Recently, theory framework of influence factors of consumers' trust in mobile commerce has gained much attention. Then a questionnaire on trust evaluation of mobile commerce is designed for reliability analysis and validity analysis on the trust evaluation scale respectively[7, 8, 9]. Due to lack of punishment to malicious recommendation from referee (nodes), enormous subjective malicious recommendation nodes are remained in network and they are searched by the next criminal opportunity constantly. This paper proposes a dynamic recommendation trust evaluation model based on mobile e-commerce environment. On the basis of the research questions above, we proposed a Fuzzy Trust Measurement(FTM)model for trust evaluation. Given the fuzzy trust definition of nodes, the model can calculate local trust with fuzzy inference and obtain recommendation from neighboring nodes. Then the recommendation will be combined with local trust after getting synthesis weight with fuzzy inference to obtain comprehensive trust of nodes finally.

II. FLOW DIAGRAM OF TRUST EVALUATION

The flow chart describes the recommended value, trust degree of recommendation and domain reliability in mobile commerce system, as shown in Figure 1. Trust depends on observation and recommendation of the third party. The design of FTM model is as follows. Firstly, it is to assess the initialized trust value of local node by observing the change in the trust factor and combine it with the fuzzy inference which is to be updated. Secondly, it is to assess the trust value of node by collect in recommendation information from other nodes. Finally, it is to assess recommendation from the local node by using fuzzy reasoning weighted with its comprehensive rights credibility from recommendation trust value, on the basis of which the recommended trust value in the synthesis assessment will form a comprehensive trust value of the system.

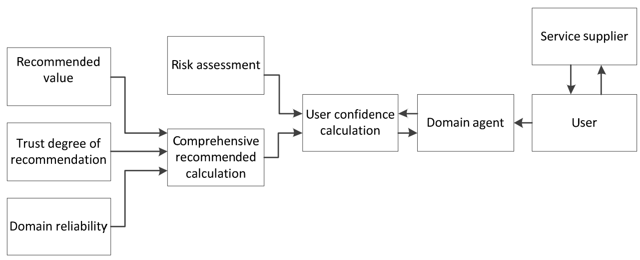

FIGURE I. FLOW DIAGRAM.

Recommendation value of trust values is indicated by vector form $E_{IT} = \left(E^{I}_{T1}, E^{I}_{T2}, E^{I}_{T3}, E^{I}_{T4}, E^{I}_{T5}\right)$. In order to cut energy waste in communication and prevent the recycle loop of the trust, it is limited between neighboring nodes without using pass iteration. The recommended trust value provided by interrelated node is referred to as a recommendation node. As shown in Figure 1, the recommendation nodes would automatically send the trust value of the local nodes that being assessed as comprehensive recommended calculation to evaluate nodes after receiving the evaluation requirement of other nodes. Then its local trust value of the node can be evaluated as a recommendation trust value to the node trust assessment. To sum up, only nodes who are the neighbor with

© 2015. The authors - Published by Atlantis Press

both evaluating nodes and have been evaluated by others can provide recommendation trust value.

Risk was assessed with a distributed algorithm in the mobile commerce, where the two adjacent nodes trust each other, and the user confidence calculation in made inassessment node, while the objects are called evaluated nodes. Therefore, the FTM model is designed as follows. Firstly, it is to assess the local nodes' trust value assessment, thenbe combined with the fuzzy inference to update it by observing the change in the trust factor. Secondly, it is to assess noderecommendation gathered from other nodes to assess the trust value of nodes. Finally, the assessment node is recommended by its local node using fuzzy reasoning with comprehensive right credibility from its recommendation trust value weights, where recommended trust value in the synthesis of the assessment is the comprehensive trust value of the whole system.

Domain agentneedsto collectrecommendation trust values and synthesizethemto an integrated trust value of the local trust value in order to improve the accuracy and robustness of trust assessment for user and service provider. Therefore the comprehensive trust value's vector form is marked as $E_{CT} = \left(E_{T1}^{C}, E_{T2}^{C}, E_{T3}^{C}, E_{T4}^{C}, E_{T5}^{C}\right)$. Node's trust value is decided by two-step process, overall weight computing and synthesis trust value.

III. Fuzzy Trust Measurement Model

In the process of quantizinglocal trust value, the observation of the trust factor is a subjective cognitive process, which is of strong fuzziness, where credibility trust factor with multiple values from different observation factors is a comprehensive assessment of nodes and weights are neededto determine a problem.

Nodes in mobile commerce are usually deployed in densely. However, due to the randomness of the distribution of nodes, there is some special circumstance that nodes might have no recommendations. In this case, the assessment directly from the neighboring node is evaluated as an integrated trustable node.

Evaluated node will be assessed on its own observations by comprehensive trust factorsof multiple nodes to quantify the value of trust result, which iscalled as a local trust value Z_{BC} ,with vector form as $Z_{BC} = \left(Z_{C1}^{B}, Z_{C2}^{B}, Z_{C3}^{B}, Z_{C4}^{B}, Z_{C5}^{B}\right)$.Quantization process of local trust value is divided into two phases, initialization phaseand update phase.

Therefore, node trustis classified as several grades. Let *x* be the node's credibility, its domain is $T_X = \{d \mid d \in [0,1]\}$.The trust classification nodes are described by five variables: "absolutely incredible", "compared unreliable", "uncertain", "less credible" and "absolutely credible". The corresponding fuzzy subset are X_1, X_2, X_3, X_4 and X_5, the corresponding membership function are $\beta_{X_1}, \beta_{X_2}, \beta_{X_3}, \beta_{X_4}$ and β_{X_5}, and according to the trust classification of nodes, the trust value of the node is represented as a vector

$$T_D = \left(r_{D_1}, r_{D_2}, r_{D_3}, r_{D_4}, r_{D_5}\right) \tag{1}$$

where(k = 1,2, …, 5) is the membership degree of the node trust category D_k.

Let the other assignment be 0, that is, Z_{BC} =(0, 0, 1, 0, 0), and the initial value $\lambda_1^*, \lambda_2^*, \cdots, \lambda_m^*$ is 0.In case of lacking prior information, assessing node cannot be trusted to determine the assessmentcondition of nodes and will be evaluated by local trust value node as anuncertain component of the assignment.After the establishment of the neighbor relationship of nodes, all nodes can be reviewed to assess the initial local trust value of the system. To reflect this subjective fuzziness, the node trust value based on fuzzy set theory is determined as shown in Figure 2.

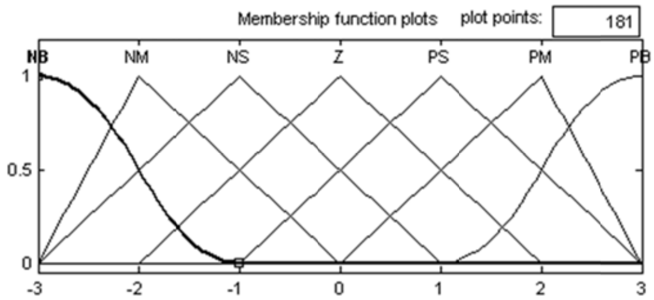

FIGURE II. FUZZY TRUST VALUE.

As we can see from Figure 2, there are 7 fuzzy trust language value, namely {NB,NM,NS,Z,PS,PM, PB}, to define different trust degree.In the mobile commerce networks, subjective fuzziness of trust evaluation nodes mainly appears fuzzy, where trust classification is based onmore value, instead of binary logic. That is to say, we could not simply classify a node into trustable or unreliable, and we should take the middle status into consideration. Trust is not either-or, but both-and, that means a node belongs to not just a category of trust, but more than one trust category in varying degrees.

IV. Algorithm of Fuzzy Trust Measurement

Suppose that there are n trust factors: $H_1, H_2, \cdots, H_n$ (j = 1, 2, …, n) can be classified as m grades: $K_{j1}, K_{j2}, \cdots, K_{jm}$. Thus thecorresponding fuzzy subsets of its membership function are $\beta_{kj1}(\varepsilon_i), \beta_{kj2}(\varepsilon_i), \cdots, \beta_{kmi}(\varepsilon_i)$,respectively, which represents the I-type trust factor. Thus, the local trust value is calculated as follows.

① Defining fuzzy inference rules. According to rule knowledge and experience of trust reasoning, the fuzzy rules of node trust factor can be gotten by derived category, the total rules isset as W.

Rule 1: if H_1isK_{j1}, and $H_2$is K_{j2}, and … and$H_n$isK_{jn}, thenX is X_1;

Rule 2:if $H_1$is K_{j1}, and H_2 is K_{j2}, and … and$H_n$isK_{jn}, thenX is X_1;

Rule W: if H_1isK_{j1}, and H_2 is K_{j2}, and … and$H_n$isK_{jn}, thenX is X_5;

②Building fuzzy implication relationship S_{k-x}. At first, it is to strike implication relations under a single fuzzy rule S_λ = (λ =1,2,…,W) with formula S_λ = $\beta^{\lambda}_{K1}(\varepsilon_1) \wedge \beta^{\lambda}_{K2}(\varepsilon_2) \wedge \cdots \wedge \beta^{\lambda}_{Km}(\varepsilon_m) \wedge \beta^{x}_{\lambda}(x)$, where $\beta^{\lambda}_{K1}(\varepsilon_1)$, $\beta^{\lambda}_{K2}(\varepsilon_2)$,…, $\beta^{\lambda}_{Km}(\varepsilon_m)$ are the first fuzzy rules under the membership functional subset. Secondly all the fuzzy comprehensive implication relations are under the rules.This rule contains multiple relationships as follows.

$$S_{k-x} = \vee^{W}_{\theta=1}\left(\beta^{\lambda}_{K1}(\varepsilon_1) \wedge \beta^{\lambda}_{K2}(\varepsilon_2) \wedge \cdots \wedge \beta^{\lambda}_{Km}(\varepsilon_m) \wedge \beta^{x}_{\lambda}(x)\right) \quad (2)$$

③Calculating thelocal credibility of every nodes. Using the actual value of the trust factor $\lambda^*_1, \lambda^*_2, \cdots \lambda^*_m$ and synthetic relationship S_{k-x}, fuzzy output of local credibility node can be gotten as formula (3)

$$\beta^{*}_{x}(X) = \vee^{W}_{\theta=1}\left(\beta^{\lambda}_{K1}(\varepsilon_1) \wedge \beta^{\lambda}_{K2}(\varepsilon_2) \wedge \cdots \wedge \beta^{\lambda}_{Km}(\varepsilon_m) \wedge \beta^{x}_{\lambda}(x)\right) \quad (3)$$

Then using the center of gravity degasification method,the credibility of the local node can be obtained, such as the formula (4)

$$X^* = COG = \int \beta^{*}_{X}(X) \cdot Xdx \,/ \int \beta^{*}_{X}(X) \cdot Xdx \quad (4)$$

④ Integratingthe trust vector of local nodes. Using the node-local credibility and membership function of each node's local trust value, the trust category can be calculated as formula (5).

$$Z_{BC} = \left(\beta_{x1}(X^*), \beta_{x2}(X^*), \beta_{x3}(X^*), \beta_{x4}(X^*), \beta_{x5}(X^*)\right) \quad (5)$$

Therefore, FTM model uses fuzzy inference trust value of local node in calculation, not only embodying the trust quantifying subjective process, but also preventing the problem of weight uncertainty of the trust factor in calculating.

V. Simulated Experiment and Analysis

Experiment is based on MATLAB.The scene is set as follows:assumingthe communication radius of each node is 25 m, and packet loss rate and packet tampering rates are set as 75% to 100%.There are 100 nodes randomly dispenser in a 100 *m*×100 *m* detection area, among which 10 nodes are set as malicious nodes.Under the collusion and strategic attack mode,the updating cycle of local trust value is assumed as 0.1*s*. The simulation resultsof fuzzy trust measurement compared with traditional crisp trust measurement are shown in Figure 3.

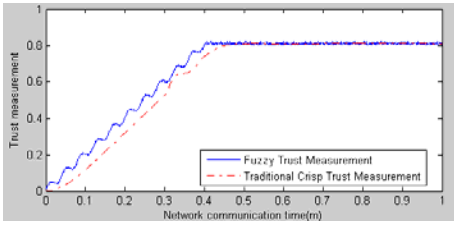

FIGURE III. TRUST MEASUREMENT RESULTS OF FTM MODEL AND TRADITIONAL CRISP MODEL.

The absolutely credible and less credible nodesare designated as malicious nodes in our experiments. We test the validity of FTM model to improve network security by observing the discovered proportion of maliciouslocalnodes, and compare them with the traditionalcrisp model. Figure 2 shows that the two found proportions of malicious nodes are different, and under the model FTM, the proportion of malicious nodes was found rise rapidly in the initialization phase of the network, and then maintained at a high level of 0.8. The reason is that FTM model definite node trust value of fuzzy and quantification fuzzy inference which ensures the accuracy of trust evaluation, and enhances the inclusive analysis of the weights and the robustness of trust assessment.

VI. Summary

Here a trust evaluation model is put forward for mobile commerce based on fuzzy mathematics, and the formal definition of the trust value of nodes is given.Therefore we can quantify the value of a local trust with the method of fuzzy reasoning and obtain recommendations from its’ neighbor nodes.Finallycomprehensive trust of thewhole system can be obtainedby trustable nodes.Future research should focused on combinedcomputing with local trust after getting synthesis weight with fuzzy inference

Acknowledgements

This research was supported by the National Natural Science Foundation of China (No. 71471102), and Key Projects of Science and Technology Research Program of Hubei Provincial Department of Education in China (Grant No. D20101203).

References

[1] Chou, Tao.An Empirical Examination of Initial Trust in Mobile Payment [J]. Wireless Personal Communications, 2014, 77(2): 1519-1531.

[2] Yan, Zheng; Liu, Conghui; Niemi, Valtteri. Exploring The Impact of Trust Information Visualization on Mobile Application Usage [J]. Personal and Ubiquitous Computing, 2013, 17(6): 1295-1313.

[3] Zhang, Ruidong; Chen, Jim Q; Lee, CaJaejung. The Effects of Location Personalization on Integrity Trust and Integrity distrust in Mobile Merchants [J]. Mobile Commerce and Consumer Privacy Concerns, 2013, 53(4): 31-38.

[4] Wang, Nan; Shen, Xiao-Liang; Sun, Yongqiang.Transitionof Electronic Word-of-Mouth Services From Web to Mobile Context: A Trust Transfer Perspective [J]. Decision Support Systems, 2013, 54(3): 1394-1403.

[5] Liu, bailing; Zheng, D; Shi, J; Zhang, L; Cloud-based Trust Establishment Protocol towards Mobile Commerce [C]. International

Conference on Computer, Networks and Communication Engineering (ICCNCE), 2013: 700-702.

[6] Liu,bailing; Wang, Weijun; Wang, Jianzong. A Negotiation Support Framework for Establishing Bilateral Trust in Mobile Commerce [J]. Information-An International Interdisciplinary Journal, 2010, 15(9): 3841-3847.

[7] Piao, Chunhui; Wang, Shuzhen; Wen, Jie. Mobile Commerce Trust Model and Its Application for Third Party Trust Service Platform [C].IEEE 14th International Conference on Commerce and Enterprise Computing (CEC), 2010:120-125.

[8] Piao, Chunhui; Wang, Shuzhen; Yang, Fengtao. Research on Trust Evaluating Model for Mobile Commerce Based on Structural Equation Modeling [C]. 9th IEEE International Conference on e-Business Engineering (ICEBE) / 8th SOAIC / 6th EM2I / 6th SOKMBI / 4th ASOC, 2012: 25-32.

[9] Bhalaji, N; Shanmugam, A. Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks [C]. International Conference on Communication Technology and System Design, 2012, 30: 881-888.