Computers, Materials & Continua CMC, vol.62, no.1, pp.123-136, 2020

Mobile Internet Mobile Agent System Dynamic Trust Model for Cloud Computing

Weijin Jiang[1, 2, 3], Yang Wang[1, *], Yirong Jiang[4, *], Yuhui Xu[1], Jiahui Chen[1], Lina Tan[1] and Guo Liang[5]

Abstract: In mobile cloud computing, trust is a very important parameter in mobile cloud computing security because data storage and data processing are performed remotely in the cloud. Aiming at the security and trust management of mobile agent system in mobile cloud computing environment, the Human Trust Mechanism (HTM) is used to study the subjective trust formation, trust propagation and trust evolution law, and the subjective trust dynamic management algorithm (MASTM) is proposed. Based on the interaction experience between the mobile agent and the execution host and the third-party recommendation information to collect the basic trust data, the public trust host selection algorithm is given. The isolated malicious host algorithm and the integrated trust degree calculation algorithm realize the function of selecting the trusted cluster and isolating the malicious host, so as to enhance the security interaction between the mobile agent and the host. Given algorithm simulation and verification were carried out to prove its feasibility and effectiveness.

Keywords: Cloud computing, mobile agent system, subjective trust, objective trust, dynamic trust management, mobile Internet.

1 Introduction

As a new Internet application business model, “Cloud computing” shields users from issues, such as data center management, big data processing, and application deployment. Through the network, users can quickly apply for or release resources according to their business needs, and pay for the resources used in an on-demand payment manner. With its economic advantages of convenient services to attract the attention of many enterprises in the IT industry, “cloud computing” is generally considered to have a huge market growth prospects. From a technical perspective, “cloud computing” has two key

[1] Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Hunan University of Technology and Business, Changsha, 410205, China.

[2] Institute of Big Data and Internet Innovation, Hunan University of Technology and Business, Changsha, 410205, China.

[3] School of Computer Science and Technology, Wuhan University of Technology, Wuhan, 430073, China.

[4] Tonghua Normal University, Tonghua, 134002, China.

[5] School of Bioinformatics, University of Minnesota, Twin Cities, USA.

[*] Corresponding Authors: Wang Yang. Email: wangyangwy25@163.com;
Yirong Jiang; Email: lxh_yyy@163.com.

points. One is the research on the distribution method of large-scale dynamic resources in resource pools; the other is the computational methods and programming methods on distributed collaborative application development platforms. The mobile agent model can realize the core idea and computing principle of mobile internet cloud computing in terms of technology, and realize the business service form of cloud computing in terms of service. However, due to the virtuality, dynamics, openness and commonality of the cloud environment, it brings great security challenges to the application of the mobile agent paradigm [Boss, Malladi, Quan et al. (2007)].

In the cloud computing environment, the problem of resource allocation of trust security domain in mobile agent system is studied [Gray, Cybenko, Kotz et al. (2012); Busi and Padovani (2009)]. It can track international cutting-edge technology, enrich the theoretical system of cloud computing and mobile agent model, and enhance the security performance of agent application system. It can also promote the application of mobile agent technology in various fields in the cloud computing environment. Therefore, it is of great theoretical and practical significance to study the security trust problem in the design of mobile agent system in cloud computing environment.

2 Related work

The trust problem of the mobile agent system has both the generality of the network trust problem and its own particularity. In 1996, Blaze et al. first proposed the concept of "Trust Management", which was used to solve the security problem of system network services. The basic idea is: trust management is to provide a secure decision framework that is suitable for network applications, open, distributed and dynamic [Blaze, Feigenbaum and Lacy (1996)]. In 1999, Povey [Povey (1999)] based on the definition of Blaze, combined with the research results of Gambetta and Abdul-Rahman et al. [Abdul-rahman and Hailes (1998); Abdul-rahman (1997)], gave a more universal concept: tust management is considered a process of acquiring, evaluating, and implementing Trust Intention.

Currently, the trust management model is generally divided into two categories. The first category is the objective rational model. It uses a rational and accurate method to express and deal with complicated trust relationships, and has objective and static management characteristics. The second category is the subjective empirical model, which considers trust to be a subjective judgment of a particular level of specific characteristics or behavior of the object. This type of trust model believes that trust is subjective, irrational, and has an empirical experience, including the specific content of trust and the division of trust levels, which is constantly modified based on changes in the outcome of object behavior.

In the Internet field, the commonly used network trust management models are PKI and PGP software packages. The European-developed ICE-TELL project combines PGP and PEM to define a new trust management model. The development of this project has further promoted the extensive research of the network trust model, and the following typical models have emerged.

Based on Reputation trust management model. For example, Derbas et al. [Derbas, Kayssi, Artail et al. (2003)] and presented an "A Coherent Trust Metric" algorithm. This algorithm uses five parameters to quantify and compare the trust level of a trusted entity.

Based on Trust Management Model Behavior. Gui et al. [Gui, Xie, Li et al. (2004)] proposed a behavior-based trust management model to allocate resources according to whether the user's historical behavior is trustworthy.

The Simple Public Key Infrastructure (SPKI) method was proposed by Carl Ellison and Bill Frantz [Jiang and Li (2007); Ellison, Frantz, Lampson et al. (1996); Ellison, Frantz, Lampson et al. (1998)], which was standardized by the IETF in 1999. The SPKI standard now in use is a mixed version of SPKII/SDSI.

The complexity of using the traditional method to solve the security problem of the mobile agent system is that it only analyzes multiple risks and multiple attacks, and the common reason that does not deeply consider the different risks is often the break of a certain trust relationship.

In Huang et al. [Huang, Tian and Huang (2015)], based on the network peer-to-peer trust model, an objective trust management model for mobile agent system is proposed. By implementing trust binding on the mobile agent and the source host, objective trust management and cross-certification are performed on the source host and the execution host.

Li et al. [Li, Lv and Cao (2002)] studied the multi-objective optimization and trust method for task scheduling in mobile cloud computing environment.

Xie et al. [Xie, Yuan, Zhou et al. (2018)] studied the trust problem in container-based cloud computing environment. Experimental simulation results show that collaborative trust assessment can solve the trust problem and improve the success rate of subsequent collaboration.

Based on the above-mentioned related trust management analysis and research, combined with our work in recent years [Jiang, Zhong, Zhang et al. (2013); Jiang, Zhang and Wang (2009); Jiang, Xu, Gu et al. (2014); Jiang, Xu and Zhang (2013); Jiang (2014)]. This paper studies the trust problem of mobile agent system by combining objective rational model with subjective empirical model. On the basis of the objective trust peer management of the mobile agent system, a dynamic management method of subjective trust is proposed, which can avoid and solve the above problems. The complexity of trust verification is reduced from the design principle. Compared with the existing PKI-based trust management model, the trust certificate is designed based on SPKI+RBAC, which reduces the complexity of trust verification. It can not only meet the requirements of trust transfer and verification of mobile agent system, but also control the attenuation of trust caused by excessive trust chain.

3 Dynamic management method of subjective trust in mobile agent system

3.1 Mobile agent system subjective trust dynamic management model

Based on the objective trust peer management model, we focus on the dynamic management method for the subjective trust demand research of the mobile agent system. Based on the interaction behavior, measure the trust status of the interactive host, and realize the dynamic management functions such as the formation, dissemination and evolution of subjective trust.

The composition of the mobile agent system supervisor trust model is shown in Fig. 1 [Jiang, Zhong, Zhang et al. (2013); Jiang, Zhang and Wang (2009)]. Bottom-up: The host

is in an open and dynamic network environment. The mobile agent platform (MAP) is located on the host, providing an Execution Environment (EE) for the mobile agent. The MAP is not necessarily unique on a host, but more than one. The subjective trust management model is located in the MAP and consists of three trust components: They are the trust formation component, the trust propagation component, and the trust evolution component. These management mechanisms provide a trust interaction context for the interaction entity, and monitor the interaction process and behavior of the entity. The trust formation component mainly implements the collection and calculation of trust data, the trust propagation component mainly implements the protocol exchange of trust data, and the trust evolution component mainly realizes the update of the trust data.

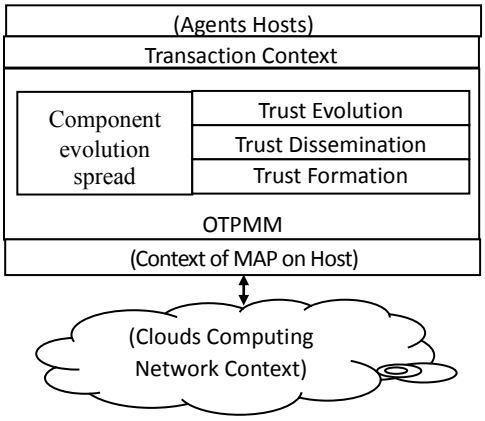

Figure 1: Subjective trust dynamic management model

3.2 "public trust" host selection

This article defines: If a third-party host H_a based only $\{H_1, H_2, ..., H_k\}$ recommendation data to calculate the extent of trusted hosts H_x, and select trusted interactive objects, the selected host will be called a "public trust" host. The "public letter" host selection algorithm provides a method for selecting a trusted interactive object for the host in the mobile agent system, especially the host newly added to the mobile agent system. If the host H_a wants to check the trustworthiness of host H_x, the host H_a sends a series of queries about the host to the third-party host $\{H_1, H_2, ..., H_k\}$. After the host H_a obtains a series of basic recommendation data, the recommended data is analyzed according to a certain algorithm, the degree of trust is calculated, and the calculation result is compared, and the host H_a selects the trusted host according to its own trust threshold.

We divide the continuous system runtime into equally spaced inspection periods, each of which is called a "time frame" and is represented by τ(τ=1, 2, ..., n). Then the interactive behavior of the interactive host is transformed into the quantitative calculation of trust degree. The Gaussian probability distribution theory is used to improve the average algorithm, and a more optimized algorithm is given. The algorithm is as follows.

Algorithm 1. Recommended trust computation algorithm.

Initialization: Let the basic data received by host H_x about host H_a be: $\{D_1, D_2, ..., D_k\}$, where: $D_i = n_1/(n_1+n_2)$, (0≤D≤1). n_1 is the number of positive interaction results about host H_x collected from M_i during the inspection period, and n_2 is the number of negative interactions.

Step 1: The data on the host recommended averaging and variance are calculated as follows:

$$\bar{D} = \frac{1}{k}\sum_{i=1}^{k} D_i \qquad S^2 = \frac{1}{k}\sum_{i=1}^{k}(D_i - \bar{D})^2 \tag{1}$$

Step 2: Order: $\mu = \bar{D}$, $\sigma^2 = S^2$, according to a Gaussian distribution theory, that $K(\mu,\sigma^2)$ use as the characteristic parameters for a random variable T, T obtained probability density functions $p(x)$, which (μ,σ^2) are called expectation and variance of the Gaussian distribution. When μ=0, $\sigma^2 = 1$, the time, T is called the standard normal distribution.

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \ (\sigma>0), \ (-\infty<x<+\infty) \tag{2}$$

Step 3: The possibility of random variable T in (-∞, v), (v, + ∞) appearing in the range can be obtained. Wherein, P (≤V) T indicates the possibility of appearing in the range of v or less, P (> v) T indicates the possibility of occurring within the range of greater than v.

$$P(\le v) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\frac{v-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx, \quad P(>v) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v-\mu}{\sigma}}^{\infty} e^{-\frac{x^2}{2}} dx$$

For a given interval value (v_1, v_2), T appears in the specified range possibilities:

$$P(v_1, v_2) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx, \ (v_1 < v_2) \tag{3}$$

Step 4: Then the variable T in the specified range (v, 1), the possibility [0, 1] appear respectively:

$$P(v,1) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx, P(0,1) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\frac{0-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \tag{4}$$

Step 5: Then calculated variables (v, 1) within the scope of the likelihood ratio in the range [0, 1] and T:

$$P_{ax}(v) = \frac{P(v,1)}{P(0,1)} = \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \Big/ \int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \tag{5}$$

Step 6: The host H_a recommended level of trust on the host H_x (0 <v <1) defined as the ratio (v) is P_{ax} (v) (0<v<1). Referred to as T_{x-rec} (v), T_{x-rec} (v)= P_{ax} (v)(0<v<1),

where v is the calculated threshold value.

Computing a set threshold v, the host H_a has the intention of candidate host interaction $\{H_{x1}, H_{x2},..., H_{xk}\}$, followed by calculation of $\{T_{x1}(v), T_{x2}(v),... T_{xk}(v)\}$, which can choose a higher level of trust list host. These hosts are selected based on recommendation after data calculation, and there is a certain degree of public trust, known as the "public trust host". If the host H_a is a newly added mobile Agent system, it is more reasonable to use this algorithm to select the interactive host. If H_a and H_x have direct interaction experience, based on direct empirical data, this algorithm needs further improvement.

3.3 Direct calculation trust

In fact, host H_a's trust evaluation of host H_x is primarily influenced by direct interaction experience. If the host H_a and the host H_x have already had experience in interacting with each other, use the algorithm given in the previous section to calculate the direct trust base data. The host H_a can obtain the trust level of the host H_x by direct experience, which is called the degree of direct trust, and is recorded as $T_{x-dir}(v)$.

The continuous system uptime is divided into equal statistical period, each study period called a "time frame", with τ (τ = 1,2, ..., k) represents. Within each time frame τ, assumptions and direct interaction $n_1 + n_2$ times, positive event n_1 times, negative event n_2 times. Definition of direct experience data calculated by the formula (6).

$$D_{ax} = \begin{cases} \frac{n_1}{n_1+n_2} (n_1+n \neq 0) \\ 0.5 (n_1+n_2=0) \end{cases} (0 \le D_{ax} \le 1)，（\tau=1，2，...n) \tag{6}$$

In k successive time frame for

$$\overline{D}_{ax} = \frac{1}{k}\sum_{i=1}^{k} D_i, \quad S_{ax}^2 = \frac{1}{k}\sum_{i=1}^{k}(D_i - \overline{D}_{ax})^2 \tag{7}$$

Order: $\mu = \overline{D}_{ax}$, $\sigma^2 = S_{ax}^2$, have K (μ, σ), based on the Gaussian probability distribution theory, can be obtained directly on the degree $T_{x-dir}^{\tau} = P_x^{\tau}(v)$ of trust in the host.

In each inspection period, the direct experience data of the host H_a to the host H_x can be collected, and the recommended data $\{D_1, D_2,..., D_k\}$ of H_x can be obtained by querying the third party $\{H_1, H_2,..., H_k\}$. Comparing the difference between the direct empirical data D_a and the recommended data $\{D_1, D_2,..., D_k\}$, the direct trust degree $\{T_1, T_2,... T_k\}$ of the recommender $\{H_1, H_2,..., H_k\}$ is adjusted. The adjustment method is: if (D_a, D_k) has a good consistency, then increase the direct trust of M_k; otherwise, the direct trust of M_k will be reduced. This adjustment has an isolated effect on maliciously recommended hosts that intentionally provide high recommendation and low recommendation values [Jiang, Xu, Gu et al. (2014); Jiang, Xu and Zhang (2013)]. The specific algorithm is as follows:

$$T_k = \begin{cases} T_k + \dfrac{(1-T_k)}{2}\left(\dfrac{\delta D_{ka}}{\bar{\delta D}_{ka}}\right), (\delta D_{ka} \le \bar{\delta D}_{ka}) \\ T_k - \dfrac{T_k}{2}\left(\dfrac{\delta D_{ka}}{\bar{\delta D}_{ka}}\right), (\delta D_{ka} \ge \bar{\delta D}_{ka}) \end{cases}, (k=1,2,...) \quad (8)$$

$$D_{ka}=|D_k-D_a|,\ \bar{D}_{ka} = \frac{1}{k}\sum_k |D_k - D_a|, (k=1, 2, \ldots) \quad (9)$$

Based on the direct trust threshold $(T_{x-dir} > T_0)$ and the recommended trust threshold $(T_{x-rec} > T_0)$, the trusted host list is selected, and the host with the bad recommendation behavior can be further analyzed by using the above algorithm.

3.4 Comprehensive calculation of trust

The accuracy of the measurement, evaluation and prediction of the trust level of the interactive host in the mobile agent system is the basis for optimizing the new management. More generally, consider both direct trust data and recommended trust data. A more reasonable algorithm is to comprehensively calculate the direct trust degree and the recommended trust degree of the obtained host H_k, and finally obtain the comprehensive evaluation result of the trust degree of the host H_a to the host H_k.The following is a "trust" comprehensive calculation process.

During the same study period, the direct trust level T_{x-dir} and the recommended trust strength T_{x-rec} are weighted and summed, where ρ is the confidence coefficient.

$$T_x=\rho T_{x-dir}+(1-\rho) T_{x-rec} (0<\rho\le 1) \quad (10)$$

The degree of trust is updated according to the algorithm given by Eq. (9). The algorithm implements two functions: First, if entity H_a repeatedly interacts with entity H_x and finds that H_x continues to maintain good behavior (affirmative event), H_x's trust degree T_x will continue to grow, tending to a maximum of 1, and if entity H_x has malicious behavior, its trust will drop rapidly; Second, if there is a large change in the degree of trust between time frames n-1 and n, this large amount of change H_x^n will have a large effect, and vice versa. $\sigma(\tau)$ known as the coefficient update control the update speed of trust.

$$T_x^{n+1} = T_x^{n-1} + \sigma(\tau)(T_x^n - T_x^{n-1}) \quad (11)$$

4 Simulation experiment analysis

The key properties and parameter selections of Eqs. (1) to (16) given in the above dynamic trust metrics and evaluation methods are verified by a series of simulation experiments [Jiang (2014); Cui, Song and Miao (2017); Li, Li and Gao (2017)].

4.1 Experimental conditions

Experiment 1 examines the algorithm of Eq. (1), and the result is shown in Fig. 2. Take host

H_a to investigate multiple interactions with H_x as an example to illustrate [Jiang, Xu and Zhang (2013)]: The more bad interactions of host H_x, the higher the value converted to the underlying trust data D_{ax}. If H_x always maintains good behavior, when the interaction time reaches τ=50 frames, the value of D_{ax} is almost equal to 1; conversely, the more bad interactions of host H_x, the lower the value converted to the base trust data D_{ax}. If the bad behavior persists, the value of D_{ax} is almost equal to 0 when the interaction time reaches τ=50 frames. If the host's H_x interaction behavior is mixed, the value of D_{ax} fluctuates around 0.5. Therefore, D_{ax} in Eq. (1) can correctly reflect the degree of behavior of H_a in the series of interactions with host H_x. When K does not understand H_x, H_a considers D_{ax}=0.5.

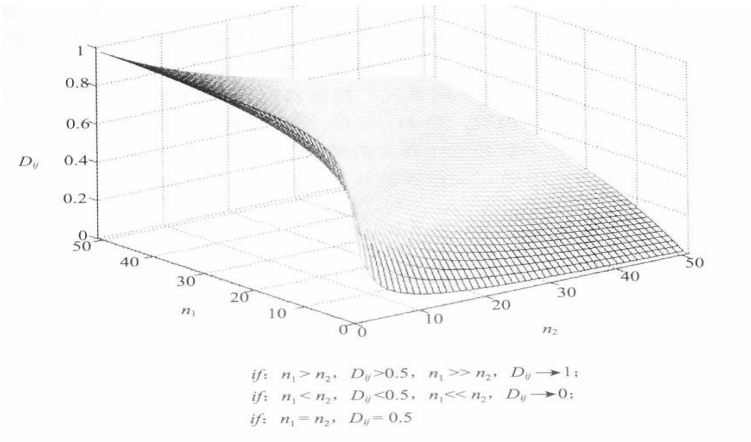

Figure 2: Verify Dij(n1, n2), (t=1, 2, …,50)

Experiment 2 examines the algorithm of Eq. (5), and the result is shown in Fig. 3. Let the trust demand threshold be T_o, and let v=T_o, you can see the change of the direct (or recommended) trust degree T_x of the host H_x when calculating the base value v (depending on the collected data is direct or recommend trust data). It can be seen that the higher the T_o value, the higher the expectation requirement for the host satisfying $T_x > T_o$, and the fewer the number of hosts satisfying the condition. For example, when the calculation base value v=trust threshold T_o=0.8, it can be seen from Fig. 3. that only the candidate host whose mathematical expectation value of the host interaction behavior μ>0.6 can be included in the trusted interaction object.

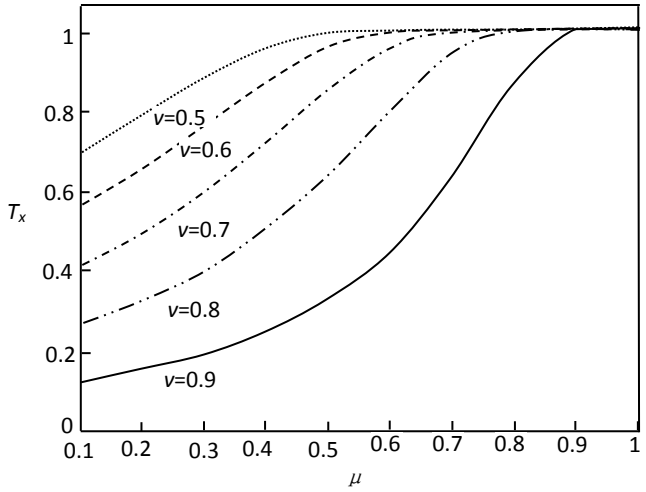

Figure 3: The relationship between the degree of Hx trust and the mathematical expectation of its behavior at different *v* values

The experimental results obtained according to the trust degree synthesis algorithm (11) are shown in Fig. 4. It can be seen that the algorithm has a slow rising fast falling feature. If host H_x continues to maintain good interaction behavior for multiple time frames, host H_x can gradually gain high trust; after obtaining high trust, H_x suddenly implements malicious behavior in the interaction to obtain illegal benefits, his trust will decline rapidly, be seen by H_a and spread through trust, so that the trusted group is isolated. If H_x wants to restore the higher trust he once had, it needs to make long-term efforts to maintain good interactions in order to restore his "trust". This main feature of the trust degree comprehensive calculation algorithm effectively suppresses the malicious behavior of the host.

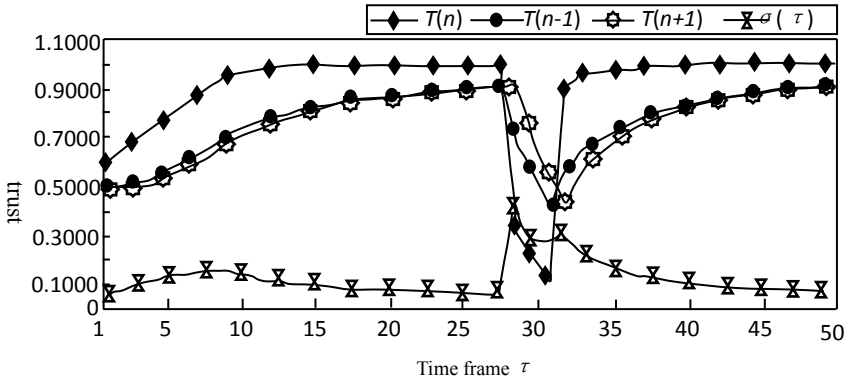

Figure 4: Changes in trust trends (w=1.5)

Eqs. (8) and (9) give an algorithm for host H_a to isolate the host M_k (k=1, 2, ...) with bad or malicious recommendation behavior based on direct empirical data on host H_x.

The simulation experiment results are illustrated as follows in Fig. 5., Fig. 6., and Fig. 7. It can be seen from Fig. 5. that the recommendation data of the recommender M_3 to the host H_x is the best with the direct empirical data of the host H_a to H_x. The recommendation data of recommenders M_1 and M_2 is inconsistent with the direct empirical data of H_a, which is much higher than and directly below the direct empirical data of H_a. Depending on the algorithm used, H_a can conclude that: M_3 is more believable, and M_1 and M_2 may be suspected of malicious recommendations.

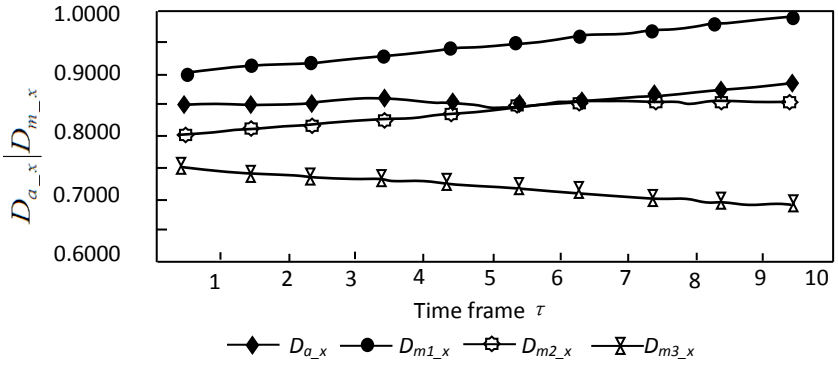

Figure 5: Comparison of direct empirical data with recommended data

Based on the direct recommendation data of H_a, the degree of deviation of the recommended data of M_1, M_2 and M_3 is further examined. and the degree of deviation from the recommended data, the results shown in Fig. 6. As can be seen from Fig. 8. in a plurality of successive cycles $|\delta D_{m2}-a|>\delta\bar{D}aver$, $|\delta D_{m3}-a|<\delta\bar{D}_{aver}$, and study within the first few cycles $|\delta D_{m1}-a|<\delta\bar{D}_{aver}$, after several cycles $|\delta D_{m1}-a|>\delta\bar{D}_{aver}$, where $\delta\bar{D}_{aver}$ is the mean difference. Depending on the algorithm used, H_a's trust in recommending host M_3 will increase, while trust in M_1 and M_2 will decrease.

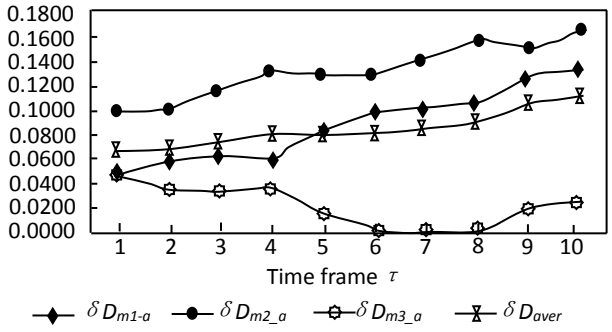

Figure 6: Differences between direct empirical data and recommended data

The effect of the difference between the direct empirical data and the recommended data on T_{m_k} is shown in Fig. 7.

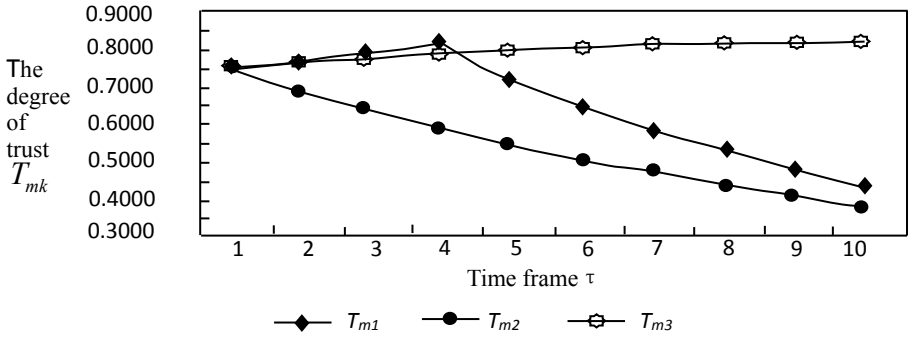

Figure 7: The effect of the difference between the direct empirical data and the recommended data on T_{m_k}

It can be seen from Fig. 7 that according to Eqs. (8) and (9), in the course of the investigation, the recommendation data of the recommender M_3 to the host H_x and the direct empirical data of the host H_a to H_x are the best. Host H_a's direct trust to him gradually increases, and the degree of improvement depends on the degree of consistency. The higher the consistency, the faster the increase; the recommendation data of recommenders M_1 and M_2 is inconsistent with the direct empirical data of H_a. Regardless of the direct empirical data far higher or lower than H_a, the direct trust of host H_a is gradually reduced. The magnitude of the decrease depends on the degree of deviation. The greater the degree of deviation, the faster the reduction. Therefore, the functions of the Eqs. (8) and (9) can effectively isolate the malicious recommendation host.

Therefore, the following conclusions can be drawn: the simulation results verify the correctness of the "public letter host selection algorithm", "isolated malicious recommender algorithm" and "trust level comprehensive calculation algorithm" given in Liu et al. [Liu, Li and Yang (2017); Hu, Liu and Hu (2017); Jiang (2016)]. It can be used to evaluate the subjective trust status of the host to be interacted in the mobile agent system, and predict the trustworthiness of the host to be interacted in the next time frame. The series of algorithms given can stimulate the trusted host and isolate the malicious host, which has the function of "punishing evil and promoting good". It can effectively manage the subjective trust dynamic management of the mobile agent system.

5 Conclusion

Divide the trust problem in the mobile agent system into objective trust and subjective trust to divide and conquer. This paper studies the problem of dynamic management of subjective trust in mobile agent system under the objective trust management framework of SPKI-based mobile agent system. The trust requirement of the entity (host or mobile agent) in the mobile agent system is analyzed, and a subjective trust dynamic

management model consisting mainly of three trust components is proposed. Among them, the trust forms a component and completes the collection of trust data; the trust propagation component completes the communication of trust and the exchange of trust data; trusts the evolution component and completes the update of the trust data. The quantitative representation method of trust in the mobile agent system is given. Based on the basic ideas of description and metric trust proposed in the Josang network trust management model, two basic concepts of Evidence Space and Opinion Space are introduced in the mobile agent system. In the fact space of the mobile agent system, the "good or bad result of entity interaction behavior" is transformed into the "level of credibility of the entity" in the concept space. Using Gaussian Probability Distribution Theory, the method of changing the degree of trust of the host in the mobile agent system is given. "Trust" is used to indicate the degree of trust that Host H_a considers Host H_x within a specified time frame in the Mobile Agent system to evaluate and predict the next secure interaction with Host H_x. A subjective trust dynamic management algorithm is proposed. Finally, through a set of simulation experiments, the feasibility of the proposed algorithm to measure the degree of host trust in the mobile agent system is verified, and the effectiveness of the trust group to improve the security of the interaction in the mobile agent system is verified.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (61772196; 61472136), the Hunan Provincial Focus Social Science Fund (2016ZDB006), Hunan Provincial Social Science Achievement Review Committee results appraisal identification project (Xiang social assessment 2016JD05), Key Project of Hunan Provincial Social Science Achievement Review Committee (XSP 19ZD1005). The authors gratefully acknowledge the financial support provided by the Key Laboratory of Hunan Province for New Retail Virtual Reality Technology (2017TP1026).

References

Abdul-rahman, A.; Hailes, S. (1998): A distributed trust model. *Proceeding of the 1997 New Security Paradigms Workshop.*

Abdul-rahmana, H. (1997): Using recommendations for managing trust in distributed system. *Proceeding of the IEEE Malaysia International Conference on Communication*.

Blaze, M.; Feigenbaum, J.; Lacy, J. (1996): Decentralized trust management. *Proceedings of the 17th Symposium on Security and Privacy.*

Boss, G.; Malladi, P.; Quan, D.; Legregni, L.; Hall, H. (2007): Cloud computing. http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf.

Busi, N.; Padovani, L. (2009): A Distributed implementation of mobile nets as mobile agents. *Proceedings of the 7th IFIP WG 6.1 International Conference on Formal Methods for Open Objective-Based Distributed Systems*, pp. 259-274.

Cui, Y.; Song, J.; Miao, C. (2017): Mobile cloud computing research progress and trends. *Chinese Journal Computers*, vol. 40, no. 2, pp. 273-295.

Ellison, C.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B. M. et al. (1996): Spki

certificate theory, request for comments 2693. *Internet Engineering Task Force.*

Ellison, C.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B. M. et al. (1998): Spki examples. *The Internet Society.*

Gray, R.; Cybenko, G.; Kotz, D. (2012): Mobile agents and atate of the art. In: J. Bradshaw, *Handbook of Agent Technology*. AAAI/MIT Press.

Guha, R.; Kumar, P.; Raghavan, P.; Tomkins, A. (2004): Propagation of trust and distrust. *Proceedings of the Thirteenth International World Wide Web Conference.*

Gui, X. L.; Xie, B.; Li, Y. N.; Qian, D. P. (2004): Study on the behavior-based trust in grid se-curity system,service computing. *IEEE International Conference*.

Hu, H. Y.; Liu, R. H.; Hu, H. (2017): Multi-objective optimization for task scheduling in mobile cloud computing. *Journal of Computer of Computer Research and Development*, vol. 54, no. 9, pp. 1909-1919.

Huang, L. S.; Tian, M. M.; Huang, H. (2015): Preserving privacy in big data: a survey from the cryptographic perspective. *Ruan Jian Xue Bao/Journal of Software*, vol. 26, no. 4, pp. 945-959.

Jiang ,W. J.; Zhang, L. M.; Wang, P. (2009): Research on grid resource scheduling algorithm based on mas coop-erative bidding game. *Science in China Series F Information Sciences*, vol. 52, no. 8, pp. 1302-1320.

Jiang, S. X.; Li, J. Z. (2007): For p2p e-commerce system based on trust mechanism reputation. *Ruan Jian Xue Bao/Journal of Software*, vol. 18, no. 10, pp. 2551-2563.

Jiang, W. J. (2014): *Research on Dynamic Modeling and Quantification of Trust Based on Multi-Agent*. Science Press.

Jiang, W. J. (2016): Multi agent system-based dynamic trust calculation model and credit management mechanism of online trading. *Intelligent Automation & Soft Computing*, vol. 22, no. 4, pp. 639-649.

Jiang, W. J.; Xu, Y. H.; Gu, H.; Zhang, L. M. (2014): Dynamic trust calculation model and credit management mechanism of online trading. *Scientia Sinica Iinformationis*, vol. 44, no. 9, pp. 100-101.

Jiang, W. J.; Xu, Y. H.; Zhang, L.M. (2013): Research on knowledge reuse dynamic evolvement model based on multi-Agent system component. *Systems Engineering -Theory & Practice*, vol. 33, no. 10, pp. 2663-2673.

Jiang, W. J.; Zhang, L. M.; Wang, P. (2009): Dynamic computing resource optimization scheduling model based on MAS collaboration mechanism. *Science in China Series F Information Sciences*, vol. 39, no. 9, pp. 977-989.

Jiang, W. J.; Zhong, L.; Zhang, L. M.; Shi, D. J. (2013): Multi-Agent dynamic collaboration model based on active logical sequence of complex systems. *Chinese journal of Computers*, vol. 36, no. 5, pp. 1115-1124.

Li, J. R.; Li, X. Y.; Gao, Y. Q. (2017): Energy saving research on mobile cloud computing in 5G. *Chinese Journal Computers*, vol. 40, no. 7, pp. 1491-1516.

Li, X.; Ling, L. (2003): A reputation-based trust model for peer to peer ecommerce communities. *Proceedings of the IEEE International Conference on E-Commerce*, pp.

275-284.

Li, X.; Lv, J.; Cao, C. (2002): Security in mobile agent system. *Ruan Jian Xue Bao/Journal of Software*, vol. 13, no. 10, pp. 1196-1205.

Liu, X.; Li, J. B.; Yang, Z. (2017): A task collaborative execution policy in mobile cloud computing. *Chinese Journal Computers*, vol. 40, no. 2, pp. 364-377.

Povey, D. (1999): Developing electronic trust policies using a risk management model. *Proceeding of the 1999 CQRE Congress.*

Xie, X. L.; Yuan, T. W.; Zhou, X.; Cheng, X. C. (2018): Research on trust model in container-based cloud service. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 273-283.

Zhang, W. L.; Guo, B.; Shen, Y.; Wang, Y. (2016): Computation offloading on intelligent mobile terminal. *Chinese Journal Computers*, vol. 39, no. 5, pp. 1022-1038.