International Journal of Computational Intelligence Systems, Vol. 7, No. 4 (August 2014), 785-795

ACO-BTM: A Behavior Trust Model in Cloud Computing Environment

Guoyuan Lin*
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, 221116, P.R. China
State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, 210046, P.R. China

Yuyu Bie
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, 221116, P.R. China
E-mail: byy2009@cumt.edu.cn
www.cumt.edu.cn

Min Lei, Kangfeng Zheng
Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China

Received 30 July 2013

Accepted 17 August 2013

Abstract

Considering trust issues in cloud computing, we analyze the feasibility of adopting ant colony optimization algorithm to simulate trust relationships between entities in the cloud and then propose a novel behavior trust model: ACO-BTM. Trust relationships between entities in cloud computing are dynamic, uncertain and hard to quantify. ACO-BTM introduces the conception of 'pheromone' and transition probability to represent behavior trust. Then, it focuses on the research of dynamic trust evaluation, time constraint and some other issues. Furthermore, a detailed algorithm process of behavior trust evaluation is given in this context. Finally, ACO-BTM is applied to cloud computing platform to simulate the establishment of behavior trust relationships. The simulation experiment verifies that trust degree change with time varies and the frequency of interactions. Compared with the other model, ACO-BTM can provide better trust recommendation services and protect against attacks of malicious nodes effectively in cloud computing environment. It is proved that ACO-BTM has good flexibility, accuracy and robustness.

Keywords: cloud computing, behavior trust, ant colony optimization, trust pheromone, heuristic pheromone

1. Introduction

Cloud computing is becoming more and more popular in both industry and academia fields. However, it is confronted with severe security issues. Many researchers are working hard in order to improve its secure environment and applications. Due to the distributivity, dynamism and uncertainty of cloud computing environment[1], centralized security mechanism is no longer meet the demand of distributed security for cloud computing. One of the main factors slowing down the development of cloud computing is the need to ensure a minimum level of trust between users and cloud computing platform. With the introduction of trust in the computer field, trust mechanism has drawn increasing attention because of its flexibility and scalability and gradually developed in various fields. Many researchers have put forward trust

*Corresponding Author: lingy@cumt.edu.cn.
Address: School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu province, China.

models for different areas, such as trust models for distributed network, P2P network, grid computing and cloud computing.

Blaze et al[3] first proposed the concept of "trust management", and provided a security decision-making framework adaptive for open, distributed and dynamic applications, to solve the safety and creditability of users and resources. A trusted cloud computing platform (TCCP)[4] was put forward by Nuno Santos in recent years. TCCP opened up the train of thought to solve trust issues in cloud computing environment. That is to prevent user's data from illegal disclosure or modification by adopting trusted computing techniques.

Inspired by ant colony optimization, a novel behavior trust model (ACO-BTM for short) is proposed in this paper according to the characteristics of cloud computing. This model focuses on the impact of interactions and time factors on trust relationships between users and cloud service providers. ACO-BTM uses the idea of pheromone perception in ants' routing process for reference and obtains direct trust value by introducing trust pheromone and heuristic pheromone. Considering the influence of time factor on the trust, trust pheromone reduction coefficient is given.

The rest of the paper is organized as follows. Section 2 outlines the related research work of trust models, especially introduces some ant colony optimization based trust models. Our proposed model ACO-BTM with a detailed description of dynamic assessment of trust relationships and time restraint is presented in Section 3. Section 4 explains the simulation experiments from two aspects: the influence of interact frequency and time factor on trust degree, the performance analysis of ACO-BTM compared with some other trust model. Finally, section 5 summarizes the whole article and points out some further research directions needed to explore in the future.

2. Related Work

2.1. *Research on trust models*

Trust in real life is a subjective concept, depending on one's experience. We can hardly describe or calculate trust using accurate models or algorithms after applying trust to network environment. Trust is the assessment of an entity's identity and trust degree of its behavior, and it is related to reliability, integrity and performance of this entity. Therefore, trust can be divided into identity trust and behavior trust. Identity trust is used to indicate the identity of an entity. The traditional access control technology usually considers identity trust, such as identity verification. After identity verification the trusted entity can access the appropriate resources. However, in network environment we cannot ensure the behavior of a user who passes the identity authentication is legal, so entities' behavior trust should be taken into account. Behavior trust is based on user's feedback to the performance of the entity the user interacts with. Hence, behavior trust is subjective, asymmetric, dynamic, and vulnerable to environmental factors[5]. Successful interactions will increase trust values, while unsuccessful interactions or no interaction occurs for a long time, trust values will decline.

Aiming at trust and collaboration issues in multi-agent system, Marsh systematically expounded the formalization of trust in 1994 which laid the foundation for the application of trust model in computer industry. Based on the conception of trust, A.Adul-Rahman divided trust into several levels and then proposed a trust computation model based on the analysis of subjective trust[6,7]. Many researchers proposed trust expressing and reasoning models to calculate trust values, and the most typical models are Beth model and Jϕsang model. Trust in Beth model[8] is composed of direct trust and recommended trust. Direct trust relationship is formed by direct interactions between two entities, while indirect trust is a trust relationship recommended by the intermediate entity between two entities that have never been interacted before. This kind of classification of trust is adopted by lots of subsequent models. Based on the probability theory, Jϕsang[9] put forward the concepts of evidence space and concept space and used it to describe and measure trust relationships. Although there's no clear distinction between direct trust and recommended trust, Jϕsang model provided the recommend operator for the computation of trust.

Many scholarly researches indicate that cloud computing trust mechanism is a key factor to guarantee the safety and credibility of cloud computing. Scholars at home and abroad have already started a more thorough analysis of trust mechanism, and put forward a variety of trust models. For example, Nuno Santos[4] designed a trusted cloud computing platform, or TCCP for short, to ensure the confidentiality and integrity in IaaS (Infrastructure as a Service) cloud computing

services. TCCP provided an abstract enclosed executive environment to user's virtual machine to ensure that privilege administrator of cloud providers cannot check or tamper with user's information. In addition, before the start of virtual machine, TCCP allowed remote users to confirm that the back-end server is running credible TCCP tasks, thereby trust certification scope is expanded to the entire service, so that users are allowed to verify whether the computational tasks run safely. Jong P. Yoon et al proposed a credible model for cloud resources based on authorization chain in Ref. 10. This model used the metadata of cloud resources and access control policy to establish authorization chains. According to the completion of authorization chains, the credibility of cloud resources can be judged. If authorization chain of a cloud resource is complete and traceable, then the resource is trusted resource. Jong P. Yoon's method is described in detail and the whole designing process is clear and concise. However, due to the super large scale of cloud resources and data, the build process of authorization chain would spend a substantial amount of time and effort. It would significantly reduce the computational efficiency and degrade performance of services in cloud computing. Wang Wei[11] built a trust model based on Bayesian theory and proposed a trusted resource scheduling algorithm on the basis of this model which is able to obtain an accurate assessment of trust with a much smaller time complexity.

2.2. *Trust based on ant colony optimization*

Ant colony algorithm is proposed by Marco Dorigo[12] inspired by the food-seeking behavior of ants. It's an algorithm used for finding the shortest path in a graph. In the foraging process of ants, it leaves behind it a trail of biochemical substrate called pheromones. The pheromone will gradually evaporate on the passage of time. The ant could recognize the existence and concentration of the pheromone, and move towards the direction with high level of pheromone concentration. That means the probability of a path to be selected is proportional to its concentration of pheromone. A path with high level of pheromone concentration will attract ants and eventually the concentration will be higher and attracts more ants, thereby forming a phenomenon of positive feedback. This is the principle of ant colony algorithm.

In Ref. 13, Punam Bedi referred to the idea of ant colony algorithm, proposed trust pheromone and established a trust based ant recommender system (TARS). In TARS, user's choice of service node is rely on trust pheromone of the node. In addition, the dynamic influence of time on trust relationships is considered. Félix Gómez Mármol also presented a dynamic trust model using ant colony algorithm. He put forward a trust based ant colony system and applied it respectively to P2P networks and wireless sensor network[14-16].

3. ACO-BTM Trust Model

3.1. *Behavior trust model*

Behavior trust relationships are generally divided into two kinds: direct trust and indirect trust relationships. Direct trust relationships are built via direct interactions based on their interactive experiences. In addition to direct interactive experiences of an entity, the establishment of direct trust relationship is also influenced by various factors, such as time, distance etc. The time factor has a very significant impact on direct trust. The degree of trust is relatively high between those entities with frequent interactions. As time goes on, trust degree will decay without interactions for a long time. Indirect trust relationship, also known as recommend trust relationship, is established via recommendation of an intermediate entity.

Behavior trust model follows a certain process, as shown in Fig. 1. The computation of direct trust and recommended trust requires taking impact factors into account. The comprehensive trust is a function of direct trust and recommended trust. The general behavior trust model will assign different weights for direct trust and recommended trust. When a user request for some resources or services, then compare the comprehensive trust degree of the resource or service provider with trust threshold. If trust value is higher than trust threshold, then the interaction will be allowed. After a successful interaction, the user will make an appropriate satisfaction evaluation of the entity, so as to update the trust value. The user will not interact with those entities with a trust value lower than trust threshold. In the reward and punishment module, users will reward entities who provide satisfied interactions by enhancing their trust value, and punish entities that do not provide proper resources or services by lowering their trust

degree. So, the trust degrees of reliable entities will be increasing higher and there will be more users choose these entities. Trust values of malicious entities will be lower and users will no longer interact with them.

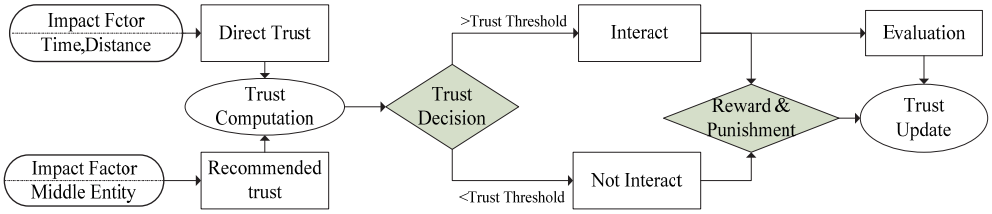

Fig. 1. General process of behavior trust model.

In cloud computing environment, users interact with the cloud computing platform so as to obtain cloud resources or services they need. In the process of interaction, users' behavior, including legal behavior or malicious behavior, will affect the confidence that cloud computing platform have in users. In addition, when providing resources or services, the timeliness of response, availability of resources and effectiveness of services and so on will affect users' trust on cloud computing platform. Moreover, trust relationships between users and cloud platform are also influenced by time factor. Trust between two entities with no interaction for a long time will gradually decrease with the lapse of time, until it is reduced to zero.

3.2. *Ant Colony Optimization, ACO*

Ant Colony Optimization, or ACO for short, is a population-based heuristic bionic evolutionary algorithm. ACO is successfully applied in solving the famous traveling salesman problem (TSP). In ACO, ants choose the optimal path according to the concentration of pheromone ants left behind. Suppose the current position of ant k is i, the transition probability of k from i to j is determined by pheromone concentration and distance. Transition probability is a function of pheromone τ_{ij} and distance d_{ij}. Among set Λ of all the accessible positions, the transition probability of ant move to position j is as follows:

$$p_{ij}^{k} = \frac{\tau_{ij}^{\alpha}\eta_{ij}^{\beta}}{\sum_{j\in\Lambda}\tau_{ij}^{\alpha}\eta_{ij}^{\beta}}. \qquad (1)$$

η_{ij} is heuristic information. It is the visibility of the path from i to j and is defined as the inverse of the distance between the two positions, that is $1/d_{ij}$. d_{ij} is the Euclidean distance of the two positions. α is the weight of pheromone τ (usually $0.5<\alpha\leq 1$). The value of α represents the importance of pheromone when choosing a path. β is the weight of heuristic information η (usually $\beta>1$). The value of β indicates the importance of distance when choosing a path.

Pheromone concentration will evaporate and disappear gradually with the passage of time. Therefore, the pheromone of a path must be updated after every time unit. Suppose ρ is the decay factor of pheromone and Q is the total quantity of pheromone ants released. In an ant colony composed of m ants, after a time unit, the pheromone updating formula is as follows:

$$\tau_{ij}(t+1) = (1-\rho)\times\tau_{ij}(t) + \sum_{k=1}^{m}\Delta\tau_{ij}^{k} \qquad (2)$$

In order to calculate $\Delta\tau_{ij}^{k}$, M. Dorigo had proposed three ant system models[17], the computation formulas are as follows:

(1) ant-quantity model

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{Q}{d_{ij}} & k \text{ passed over rout ij in the time unit } (t,t+1) \\ 0 & Otherwise \end{cases} \qquad (3)$$

(2) ant-density model

$$\Delta\tau_{ij}^{k} = \begin{cases} Q & k \text{ passed over rout ij in the time unit } (t,t+1) \\ 0 & Otherwise \end{cases} \qquad (4)$$

(3) ant-cycle model

$$\Delta\tau_{ij}^{k}=\begin{cases}\dfrac{Q}{L_k} & k \text{ passed over rout ij in this cycle}\\ 0 & Otherwise\end{cases} \quad (5)$$

Following conclusions are reached by simulation and experimental analysis of parameters in ant colony models above according to Ref. 18: 1) the optimal parameters of ant-cycle model are: $\alpha=1,\beta=5,\rho=0.5$; 2) the optimal parameters of ant-density model are: $\alpha=1,\beta=10,\rho=0.9$; 3) the optimal parameters of ant-quantity model are: $\alpha=1,\beta=5,\rho=0.999$.

In cloud computing environment, trust degree between interacted entities is similar to the pheromone in ant colony algorithm. For instance, cloud users tend to choose entities with high credibility to provide resources or services and the ants always select path with high level of pheromone concentration. The degree of trust increases as the number of interactions enhance. This is similar to the increase of pheromone. Furthermore, both pheromone concentrations in ant colony and trust degree in cloud computing decrease over time.

Ant colony optimization is a population intelligent problem solving method, and it adopts the distributed positive feedback parallel computing system. ACO is suitable for distributed feedback systems without a central control unit, such as cloud computing system. Furthermore, ACO is easy to combine with other methods, and has strong robustness. Therefore, it is feasible to apply ACO to the field of trust management in cloud computing environment.

3.3. *ACO-BTM trust model*

In cloud computing, entity's trust is subjective. So the degree of trust is unable to be described by deterministic numerical values. Trust is not only based on the results of interactions, but also influenced by time and distance. The routing choice of ants in ant colony algorithm is similar to user's selection of entity, so ACO can be used to solve trust computation problems in cloud computing. However, cloud computing system has its own characteristics. ACO is not suitable for direct application in the cloud computing environment, so some proper adjustment have to be made. For instance, transition probability in ACO algorithm can be seen as the trust value of cloud computing resource or service providers. Define a variable which is similar to pheromone to describe the trust pheromone in cloud computing environment. Trust pheromone represents the basic attribute of direct trust between users and entities. In ACO algorithm, except for the influence of pheromone concentration on ants' routing behavior in the process of foraging, the distance of the path is also an influential factor. Heuristic information is defined as the inverse of the distance. While in cloud computing environment, user's choice of entity is not only influenced by the behavior trust degree of an entity, the distance or time of data transportation between users and entities should also be considered. Therefore, a variable similar to heuristic information should be given and represent the distance or time of data transportation between users and entities.

Considering the above factors, this paper puts forward a behavior trust model based on ant colony optimization (ACO-BTM). In this model, trust relationships between users and resources or services providers will change dynamically with the change of interactive frequency and time. First, calculate trust values using ant colony algorithm. Second, recommend more reliable cloud resources or services for users. At last, a dynamic behavior trust model in cloud computing environment is established. In ACO-BTM model, trust of an entity is described by trust degree. Trust degree between two entities will increase with the accumulation of interactions. Trust between two entities with no interaction for a long time will gradually decrease with the lapse of time, until it is reduced to zero.

3.3.1. The definition of trust relationships

There are multiple nodes providing resources or services for users in cloud computing environment. The environment and size of cloud computing network have been in a dynamic changing state. Thus the interactions and trust relationships between users and resource or service providers are complicated. In order to describe trust relationships conveniently and concisely, the number of nodes in the cloud computing environment is defined as m, and the number of nodes will change dynamically over time.

When users request for cloud resources or services, the credibility of an entity should be fully considered except for its own ability. Users tend to choose entities with higher trust degree to provide resources and

services. According the history behaviors of an entity and time factor, the degree of trust is defined as follows.

Definition 1 (Trust Degree): Trust degree represents the tendency which entity the user would choose to interact. At time t, trust degree between the user u and entity e is expressed as $T_{u,e}(t)$, where $T_{u,e}(t) \in [0,1]$. $T_{u,e}(t) = 1$ represents that user u trusts entity e completely. $T_{u,e}(t) = 0$ means that user u does not trust entity e at all. Trust degree is composed of direct trust and recommended trust.

$T_{u,e}(t)$ is a function of interactions and time. If user u is interacted with entity e at time t, which means that user u requested for resources or services of entity e at time t and e provided u resources or services it asked for. After the interaction, if user u is satisfied, then trust between u and e will increase. Meanwhile, trust degree between the user and any other entity will decrease over time. No interaction happens between the user and some entity for a long time, trust will be reduced to zero. Then the user does not trust this entity any more.

Definition 2 (Direct trust): Direct trust relationship is built through direct experience of interactions between the user and entity. Direct trust degree is related to interactions and time factor. The more the user interact with the entity, the higher its degree of direct trust between them. Direct trust is represented symbolically by Dt. If the user has never interacted with the entity, then Dt is usually set to zero. At time t, user u's direct trust towards entity e is formulized as $Dt_{u,e}(t)$.

Definition 3 (Trust pheromone): Trust pheromone, formulized as Tp, is a primary cognition of direct trust degree between the user and the entity. At time t, user u's trust pheromone towards entity e is represented by $Tp_{u,e}(t)$. At the initial moment, the value of trust pheromone is generally set to zero, that is $Tp_{u,e}(0) = C$ (C is constant). Initially, if direct trust degree is zero, then the value of trust pheromone must be zero too. The formula is as follows: $Dt_{u,e}(t) = 0 \Rightarrow Tp_{u,e}(0) = 0$.

Definition 4 (Heuristic pheromone): Heuristic pheromone, formulized as Hp, is user's cognitive information about the entity. User's cognitive information is the Euler distance between the user and the entity. At time t, user u's heuristic pheromone towards entity e is represented by $Hp_{u,e}(t)$. The computation formula of heuristic pheromone is as follows:

$$Hp_{u,e}(t) = \frac{1}{d_{u,e}} \tag{6}$$

Both trust pheromone in definition 3 and heuristic pheromone in definition 4 together make up the direct trust relationship between the user and the entity. In ACO algorithm, the routing choice of ants is represented by transition probability. While in cloud computing, user's choice of resource or service providers is expressed by direct trust degree. Therefore, At time t, user u's direct trust towards entity e is formulized as follows:

$$Dt_{u,e}(t) = \frac{Tp_{u,e}(t)^{\alpha} Hp_{u,e}{}^{\beta}}{\sum_{i \notin E} Tp_{u,i}(t)^{\alpha} Hp_{u,i}{}^{\beta}}, \tag{7}$$

Where α is the weight of trust pheromone between user u and entity e, β is the weight of heuristic pheromone. E is a set of user-selectable entities. Here $E = \{1,2,\cdots,m\}$.

Definition 5 (Recommended trust): Recommended trust, or Rt, is recommended by some intermediate entity. At time t, recommended trust which the intermediate entity k gives the user u about entity e can be described as $Rt^{k}_{u,e}(t)$. The following formula shows a calculation method of recommended trust.

$$Rt^{k}_{u,e}(t) = Dt_{u,k}(t) \times Dt_{k,e}(t) \tag{8}$$

Actually, there is more than one intermediate entity which could provide the user with recommended trust. Different intermediate entities have different significance on trust values. Entities with higher degree of direct trust usually give more credible recommended trust values. Hence, when calculating the recommended trust, these entities should be given greater weights. Suppose w_k is the weight of measuring the importance of intermediate node k [19], and $\sum_{k=1}^{n} w_k = 1$. Intermediate entity k belongs to set N, and $N = \{1,2,\cdots,n\}$. At time t, user u's recommended trust towards entity e is expressed as follows:

$$Rt^{N}_{u,e}(t) = E(\sum_{k=1}^{n} w_k Rt^{k}_{u,e}(t)) \tag{9}$$

Trust between a user and an entity consists of two parts, direct trust and recommended trust. Cloud computing security management center will assign different weights to them. δ_1 is the weight of direct trust and δ_2 is the weight of recommended trust. Trust is calculated as follows:

$$T_{u,e}(t) = \delta_1 \times Dt_{u,e}(t) + \delta_2 \times Rt^N_{u,e}(t) \quad (10)$$

3.3.2. The updating of trust relationships

Trust pheromone between entities will be gradually reduced over time; therefore, we need to make updates of trust pheromone timely. The updating formula of trust pheromone is as follows:

$$Tp_{u,e}(t+1) = (1-\rho)Tp_{u,e}(t) + \Delta Tp_{u,e}(t,t+1) \quad (11)$$

Where, ρ is the decay factor of trust pheromone. $\Delta Tp_{u,e}(t,t+1)$ represents the increment of trust pheromone in the time period of $(t,t+1)$.

$$\Delta Tp_{u,e}(t.t+1) = \begin{cases} \dfrac{1}{\dfrac{1}{1-\frac{1}{5}Tp_{u,e}(t)}+1}, & \textit{If user u interacts with entity e at time t} \\ 0 & \textit{Otherwise} \end{cases} \quad (12)$$

According to deterministic theory, the following formula defines transitive relations of trust between the user and the entity.

$$T_{i,i+2}(t) = T_{i,i+1}(t) \times T_{i+1,i+2}(t) \quad (13)$$

3.3.3. The algorithm process of ACO-BTM

ACO-BTM describes the dynamic trust relationships between users and the entities using the computing method of pheromone in ant colony algorithm. The detailed algorithm process is as follows:

(i) The initialization of adjacency graph

A user requests access to a resource or a service in cloud computing platform, all the entities which could provide such resource or service and the user make up an adjacency graph. Initially at time 0, or when $t = 0$, suppose trust threshold is R. Each path has an initial trust pheromone, $Tp_{u,e}(0) = C$ (C is constant). In adjacency graph, suppose the number of all the entities including the user is m. Trust pheromones $T_{u,e}(0)$ in this graph form an initial adjacency matrix with m rows and m columns.

(ii) Calculate trust degree between user u and entity e at time t.

(a) If there exists direct interactions between user u and entity e, $Tp_{u,e}(t)$, $Hp_{u,e}(t)$, $Dt_{u,e}(t)$ can be calculated using Eq. (6) and (7);

(b) If there is no direct interaction between user u and entity e, $Rt^E_{u,e}(t)$ can be obtained using Eq. (8) and (9); At last we can get trust degree $T_{u,e}(t)$ according to Eq. (10) and some related parameters.

(iii) Comparing trust degree $T_{u,e}(t)$ with trust threshold R.

(a) If $T_{u,e}(t) \geq R$, then user u interacts with entity e. After the interaction, user u will give an evaluation of satisfaction about entity e;

(b) If $T_{u,e}(t) < R$, user u does not interact with entity e and continues to search for an entity with a higher trust degree to interact with.

(iv) If user u has a successful interaction with entity e at time t, after a time unit, trust pheromone will be updated as:

$$Tp_{u,e}(t+1) = (1-\rho)Tp_{u,e}(t) + \frac{1}{\dfrac{1}{1-\frac{1}{5}Tp_{u,e}(t)}+1} \quad (14)$$

If user u didn't interact with entity e at time t, after a time unit, trust pheromone will be readjusted as $Tp_{u,e}(t+1) = (1-\rho)Tp_{u,e}(t)$. In the meantime, update the adjacency matrix of trust pheromone based on the results of the above calculation.

(v) After the updating of trust pheromone adjacency matrix, readjust values of direct trust, and then update trust degrees.

4. Experiments and Performance Analysis

In order to make a deep understanding of trust influential factors, analyze the relations between entity's trust degree and its behavior in cloud computing environment, and expound the rationality and validity of ACO algorithm in the application of cloud computing trust management, experiments are performed to verify the impact of ACO-BTM model on success rates of interactions and prove the validity of this model.

4.1. *Experimental environment settings*

Hadoop is an open source software which can realize large-scale distributed computing, and is widely used in the field of cloud computing. Therefore, experiments in this paper are running on Map/Reduce platform in Hadoop. In order to verify the validity of ACO-BTM model and find how the trust pheromone change with entity's behavior and time variation, the settings of experimental network environment and interaction scenarios with the goal of closing to real, random and complex networks are as follows.

The purpose of Experiment 1 is to verify the impact of entities' behavior and time factor on trust degree. It doesn't require large amounts of data in this experiment, so only a small number of nodes are simulated. Experiment 2 aims at demonstrating the validity of ACO-BTM model and needs a more complex and dynamic network. So a dynamic network environment with 100-700 nodes is simulated in our lab, so as to compare ACO-BTM model with TACS model [14] from the perspective of interactive success rate and anti-attack capability.

The settings of parameter α , β , ρ has a great influence on the performance of ant colony algorithm. According to Ref. 18, the optimal parameters setting of ant-cycle model is more suitable for our model, so we choose $\alpha = 1, \beta = 5, \rho = 0.5$ in our experiments.

4.2. *Experimental results and performance analysis*

Experiment 1: The influence of entities' behavior and time factor on trust degree

In cloud computing environment, behavior information of an entity and time factor will definitely affect the entity's trust degree. Entity's successful interactive behavior will have a positive impact on trust and failure of interactive behavior will lower the degree of trust. The impact of time on the degree of trust between entities is that trust will gradually decrease over time. For further understanding of the influence of entity's behavior and time on trust degree, experiment must be done and the results will show the extent of their impact. On the Map/Reduce platform of cloud computing environment, five nodes are simulated, and these five nodes are A, B, C, D and E. Here the number of nodes is 5, that is $m = 5$. Trust relationships between the five nodes are initialized by Fig. 2. The corresponding adjacency matrix is as follows:

$$\begin{bmatrix} 1 & 0.5 & 0 & 0 & 0.1 \\ 0.5 & 1 & 0.4 & 0 & 0.7 \\ 0 & 0.4 & 1 & 0.2 & 0.3 \\ 0 & 0 & 0.2 & 1 & 0.2 \\ 0.1 & 0.7 & 0.3 & 0.2 & 1 \end{bmatrix}$$

The initial undirected adjacency graph in Fig. 2 is in an unstable state. According to trust transitive calculation method in Eq. (13), trust degree between the nodes could be adjusted. For example, there are four simple paths between node A and C: ABC, AEC, AEBC and AEDC. According to Eq. (13), trust degree between node A and C should be adjusted as: max (0.2, 0.03, 0.028, 0.004) =0.2. We can also adjust the degree of trust between the other nodes in the same way. The adjusted matrix is as follow.

$$Tp_{u,e}(t) = \begin{bmatrix} 1 & 0.5 & 0.2 & 0.07 & 0.1 \\ 0.5 & 1 & 0.4 & 0.14 & 0.7 \\ 0.2 & 0.4 & 1 & 0.2 & 0.3 \\ 0.07 & 0.14 & 0.2 & 1 & 0.2 \\ 0.1 & 0.7 & 0.3 & 0.2 & 1 \end{bmatrix}$$

As mentioned, the changes of rust pheromone between nodes along with interactions and time factor can be further analyzed in the present example. In a time unit, if none of the nodes interact with each other, then trust pheromone matrix will be updated after the first time unit as follows. Here the parameter ρ of decay factor equals to 0.5.

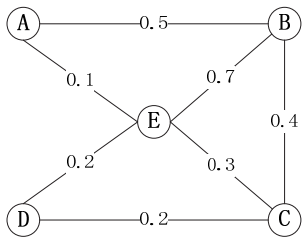

Fig. 2. The initial undirected adjacency graph

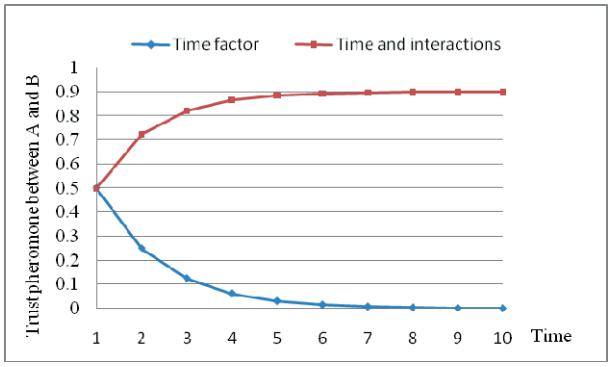

Fig. 3. Variation of trust pheromone with time and interactions between A and B.

$$Tp_{u,e}(2t) = \begin{bmatrix} 1 & 0.25 & 0.1 & 0.035 & 0.05 \\ 0.25 & 1 & 0.2 & 0.07 & 0.35 \\ 0.1 & 0.2 & 1 & 0.1 & 0.15 \\ 0.035 & 0.07 & 0.1 & 1 & 0.1 \\ 0.05 & 0.35 & 0.15 & 0.1 & 1 \end{bmatrix}$$

We can observe that the matrix above doesn't need any adjustments. If node A and B have a successful interaction in the second time unit, then trust pheromone between node A and B will be updated according to Eq. (11) and Eq. (12) as follows.

$$\begin{aligned} Tp_{A,B}(3t) &= (1-\rho)Tp_{A,B}(2t) + \Delta Tp_{u,e} \\ &= 0.5 \times Tp_{A,B}(2t) + \frac{1}{\frac{1}{1-\frac{1}{5}Tp_{A,B}(2t)} + 1} \\ &= 0.612 \end{aligned}$$

The adjacency matrix of the undirected graph could be readjusted according to trust pheromone updating method shown above.

$$Tp_{u,e}(3t) = \begin{bmatrix} 1 & 0.612 & 0.545 & 0.516 & 0.522 \\ 0.612 & 1 & 0.590 & 0.531 & 0.657 \\ 0.545 & 0.590 & 1 & 0.545 & 0.567 \\ 0.516 & 0.531 & 0.545 & 1 & 0.545 \\ 0.522 & 0.657 & 0.567 & 0.545 & 1 \end{bmatrix}$$

Furthermore, according to Eq. (7), (10) and the values of parameters, the changes of adjacency matrixes of both direct trust and comprehensive trust on the lapse of time can be obtained.

Table 1. Variation of trust pheromone between A and B with time and interactions.

Time	Tp_{A,B_1}	Tp_{A,B_2}
1	0.5	0.5
2	0.25	0.724
3	0.125	0.823
4	0.063	0.865
5	0.032	0.886
6	0.01563	0.89433
7	0.00781	0.89806
8	0.00391	0.89969
9	0.00195	0.90042
10	0.00098	0.90073

Simulation experiments on cloud computing platform describe the variation of trust degree from two aspects, the variation with time and interactive frequency. The interactions between node A and B are taken as an example. The variation of trust between node A and B with time and interactive frequency will be calculated according to the proposed ACO-BTM model. As shown in Fig. 3, the blue line indicates the variation of trust pheromone between A and B merely with the time. In fact, trust relationships between users and various entities are often affected by time as well as interactive frequency. Therefore, both time and interactive frequency are taken into account in this paper. The red line expresses the variation of trust pheromone between A and B with the influence of time and interactions. Suppose that only one interaction happens in a time unit.

As Fig. 3 shows, the initialization of trust pheromone between A and B is 0.5. When trust pheromone is only influenced by time factor, the values of trust pheromone between A and B will decrease rapidly over a period of time until it gets close to zero at the eighth time unit. This shows that time factor has a significant impact on trust degrees, and once the two entities do not interact for a long time, the value of trust will drop to zero. When two entities interact with each other every time unit, trust pheromone will increase, and the increment is greater than the amount of pheromone decay with time. Therefore, the red line is on the rise. Due to the range of trust pheromone is [0,1], the maximum value of trust pheromones is always no more than 1.

Experiment 2: The performance comparison between ACO-BTM and TACS

TACS model is proposed in Ref. 14 which used ant colony algorithm to solve the problem of trust management in P2P networks. As shown in Fig. 4, the success rate of TACS model is lower than ACO-BTM model in the initial stage. The reason is that the number of nodes and users in cloud computer network is changing all the time. Although the interactive success rate of TACS in static network is up to 96%, success rate of TACS in dynamic network is relatively lower than ACO-BTM model. However, with the increase of interactions, both ACO-BTM model and TACS model can interact with nodes with a higher trust degree using ant colony optimization algorithm, thereby improving success rate of their interactions. General trust models will inevitably encounter with malicious recommendation problems. TACS model doesn't have corresponding measures to deal with malicious recommenders, while ACO-BTM model takes full account of the recommended entities' trust degree. ACO-BTM chooses an entity with a higher trust degree as the recommended entity, thus reducing the attacks caused by malicious entities.

5. Conclusions

The rapid development of cloud computing have caused public concern of trust issues between the user and cloud platform. This article focused on trust issues of cloud resource or service providers, referred to the concept of pheromone in ant colony algorithm and proposes ACO-BTM model. This model focused on the dynamic evaluation method of behavior trust, which used trust pheromone and heuristic pheromone to describe direct trust. The comprehensive trust degree was a function of direct trust and recommended trust. Finally, cloud computing platform was built to perform simulation experiments. The results of experiments verified the variation of trust degree with time and interactions. The comparison with some other model confirmed the validity and robustness of ACO-BTM model.

Acknowledgements

This paper is supported by the Opening Project of State Key Laboratory for Novel Software Technology of Nanjing University, China (Grant No.KFKT2012B25), National S&T Major Program of China (No.2011ZX 03002-005-01), and the Fundamental Research Funds for the Central Universities (No. BUPT2013RC0308).

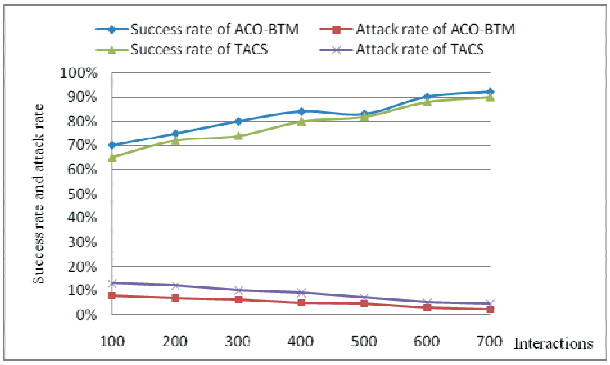

Fig. 4. The performance comparison between ACO-BTM and TACS.

References

1. Zhumu Wen, Research on dynamic trust and access control mechanism in multi-domain interoperation environment. *Huazhong University of Science and Technology*, (2008).
2. S. P. Marsh, *Formalizing Trust as a Computational Concept* (Scotland: University of Stirling, 1995).
3. M. Blaze, J. Feigenbaum and J. Lacy, Decentralized trust management. *Proceedings of the 1996 IEEE Symposium on Security and Privacy* (Los Alamitos, USA, May1996), pp. 164-173.
4. N. Santos, K. P. Gummadi, and R. Rodrigue. Towards trusted cloud computing, *In Proc. of the 1st USENIX Workshop on Hot Topics in Cloud Computing* (Berkeley, CA, USA, 2009).
5. S. Ries, J. Kangasharju and M. Muhlhauser, A classification of trust systems, *LNCS 4277/2006*. (Berlin: Springer), pp. 894-903.
6. A.Abdul-Rahman and S.Halles, A distributed trust model. *New Security Paradigms Workshop'97* (1997), pp.48-60.
7. A. Abdul-Rahman and S.Hailes, Using recommendations for managing trust in distributed systems. *Proceedings of the IEEE Malaysia International Conference Communieation'97(MICC'97)*, (Kuala Lumpur, IEEE PRESS,1997).
8. T.Beth, M.Boreherding and B.Klein, Valuation of trust in open networks. *In Proceedings of the European SymPosium on Research in Computer Security* (Springer-Verlag, Brighton UK, 1994), pp.3-18.
9. Jϕsang A, A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3), (2001), pp. 279-311.
10. Jong P. Yoon and Z. Chen, Using privilege chain for access control and trustiness of resources in cloud computing. *The 2nd International Conference on Networked Digital Technologies. JUL 07-09*, (2010).
11. Wang Wei and Zeng GuoSun, Trusted dynamic level scheduling based on bayesian trust model. *Science in*

China Series F-Information Sciences, 50 (3), (2007), pp. 456-469.
12. Colorni A, Dorigo M and Maniezzo V, Distributed optimization by ant colonies, *Proceeding of the First European Conference Artificial Life* (Paris: Elsevier Publishing, 1991), pp.134-142.
13. Punam Bedi and Ravish Sharma, Trust based recommender system using ant colony for trust computation. *Expert Systems with Applications*, 39 (2012), pp.1183–1190.
14. Félix Gómez Mármol, Gregorio Martínez Pérez and Antonio F. Gómez Skarmeta, TACS, a trust model for P2P networks, *Wireless Pers Commun* 51, (2009), pp.153–164.
15. Félix Gómez Mármol and Gregorio Martínez Pérez, Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommun Syst*, 46 (2011), pp. 163–180.
16. Félix Gómez Mármol, Gregorio Martínez Pérez and Javier G.Marín-Blázquez, META-TACS: a trust model demonstration of robustness through a genetic algorithm, *Intelligent Automation and Soft Computing*, 17(1), (2011), pp. 41-59.
17. M Dorigo, V Maniezzo and A Colorni, The ant system: optimization by a colony of cooperating agents, *IEEE Transactions on Systems, Man, and Cybernetics Part B*, 26 (1), (1996), pp.29 - 41.
18. Ye Zhiwei and Zheng Zhaobao, Research on the settings of parameter α, β, ρ in ant colony algorithm, *Journal of Wuhan University: Information Science.* 29(7), (2004).
19. Wu Hui, Yu Jiong and Yu Feiran. Dynamic access control algorithm based on trust model in cloud computing, *Computer Engineering and Applications*, 48(23), 2012, pp.102-106.