Journal of Theoretical and Applied Information Technology
28th February 2013. Vol. 48 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DISCRETE MARKOV CHAIN MODEL FOR REPUTATION ESTIMATION OF UNSTRUCTURE P2P NETWORK

HE CHAOKAI*, WU MENG

[1]College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
[2]College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing , China
Corresponding author. Email: chaokaih@hotmail.com

ABSTRACT

Building trust relationships between peers is an important and difficult part in the security needs of P2P network without a central server. P2P reputation system has been introduced which collects locally generated peer feedbacks and aggregates them to yield global reputation scores. Most P2P applications on the Internet are unstructured, without fast hashing and searching mechanisms, how to perform efficient reputation estimation is a major challenge on unstructured P2P computing. This work thus proposes a two-step reputation estimation approach for the unstructured P2P network. First, a Markov chain model is proposed to determine the reputation value for each one-hop neighbors. A peer's reputation value (RV) is analyzed from its previous trust manner in this group. The proposed trust model is proven as an ergodic Continuous-Time Markov Chain model. Second, a peer with the highest RV of a group will be selected as the central authentication(CA) server. For increasing reliability, the peer with the second highest RV will be selected as the backup group leaser(BCA) that will take over CA when CA fails. The procedures of the peer's RV are detailed. Numerical results indicate that the analytical RV of each peer is very close to that of simulation under various situations.

Keywords: *Discrete Markov Chain, Reputation Estemination, Unstructure P2P Network*

1. INTRODUCTION

A peer-to-peer (P2P) network is a computer network that does not have fixed clients and servers but a number of peers that function as both clients and servers to the others. P2P networks bring about many benefts, such as aggregating resource, cost sharing/reduction, utilizing spare resource, enhancing scalability/reliability, assuring anonymity/privacy in resource sharing, and being adaptive to dynamic environments[1]. These benefts are demonstrated in a wide range of applications, including distributed computing, file sharing, multicasting, collaborating platform, search engines, agent based systems, awareness systems, mirror systems, naming systems, etc. P2P networks are highly popular due to profitable and satisfying nature of the interactions.

P2P network's open and decentralized property makes them extremely susceptible to malicious users spreading harmful content like viruses, fake files or just wasting others' resources. To combat malicious peers and encourage resource sharing among peers, reputation (From the Oxford dicionary, reputation is the beliefs or opinions that are generally held about someone or something) management is essential for peers to assess the trustworthiness of others and to selectively interact with more reputable ones. Without an efficient reputation management facility, peers may hesitate to interact with unknown peers due to the concern of receiving corrupted or poisoned files or being exploited by malwares. Furthermore, identifying trustworthy peers is especially necessary in commercial P2P applications, such as P2P auctions, trusted content delivery, pay-per-transaction, and P2P service discovery. The mechanism through which online reputations are managed is extremely important for evolution and acceptance of these P2P services[2].

In traditional reputation systems afer transaction, the peer will rate the other according to its experience. The reputation system computes the global reputation score of a peer by aggregating the local rates from those who have interacted with this peer. peers are able to make informed decisions about which peers to trust. through making the global reputation scores publicly available, The P2P reputation systems is currently receiving a lot of attention. In an open and decentralized P2P system, there is no centralized authority to maintain and distribute reputation data. Instead, P2P reputation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

systems calculate the global reputation scores by aggregating peer feedbacks in a distributed manner .Most proposed reputation aggregation scheme, e.g., PowerTrust [3], EigenTrust [4] and PeerTrust [5] rely on the DHT mechanism to achieve scalability in aggregating and managing reputation data. However, the P2P architectures that are most prevalent in today's Internet are decentralized and unstructured, e.g. Gnutella, Kazaa and Freenet. there exists no specific reputation systems for unstructured P2P network. R Zhou Although in general any networking. Without embedded fast hashing or searching mechanism, perform efficient reputation aggregation is the major challenge in unstructured P2P networks.

GossipTrust offers the very first attempt to extend the gossip protocol for reputation aggregation in P2P networks without any structured overlay support. GossipTrust is shown very fast in aggregating local trust scores into global reputation scores. The major innovations in GossipTrust development are summarized in three aspects: fast gossip-based aggregation algorithms, efficient reputation storage with Bloom filters, and secure communication with identity-based cryptography.

Ebay[6], taobao[7] have successes in reputation aggregation which with a central authentication server. If Unstructured P2P network has a central authentication server, that will be easily to finish the reputation estimation process. To achieve the goal, we proposes a two-step reputation estimation approach for the unstructured P2P network based on dividing the P2P network into several groups . First, a Markov chain model is proposed to determine the reputation value for each one-hop neighbors. A peer's reputation value (RV) is analyzed from its previous trust manner in this group. The proposed trust model is proven as an ergodic Continuous-Time Markov Chain model. Second, a peer with the highest RV of a group will be selected as the central authentication(CA) server. For increasing reliability, the peer with the second highest RV will be selected as the backup group leaser(BCA) that will take over CA when CA fails.

The rest of this paper is organized as follows. Section 2 defines the network model. Next, the proposed Markov chain model for the reputation estimation is explained in Section 3. Section 4 presents the numerical results by the Markov chain analysis and simulations. Finally, conclusions and areas of future research are given in Section 5.

2. NETWOKR MODEL

In this section, we define a network model of a unstructured P2P network. Serval important performance metrics, including the average RV of analysis and simulation, and the number fo times a peer acted as a CA are then adopted to evaluted the proposed approach.

We model a P2P network as a graph, G=(V,E) ,which consists of a set of peers, V, and a set of links, E. Transactions session consists four parameter: a source peer s, a group of receivers R, a group ID g and a CA peer CAg of this group. In addition, $|R_g|$ denotes the number of the number of th group g and T denotes the group set of the P2P network. Each peer in a group g has a RV table used to store two type RV: 1) the group members' RV, and 2) the RV of 1-hop neighbor peers. The RV table is exchanged among group members. Finally, the group RV table could be determined, in which $RV_i(j)$ denotes the RV of peer j evaluated by peer i. An example of P2P network is indicated in Fig.1.

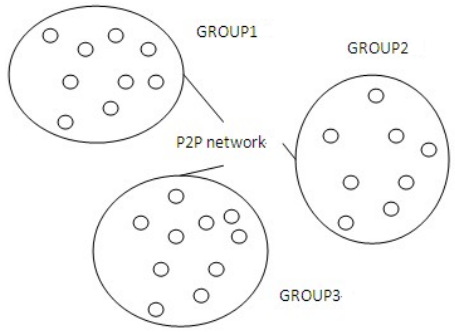


Fig.1 An example of P2P network

Two performance metrics: 1) each peer's analytic and simulation RV, and 2) the number of times a peer acted as a CA (or BCA) peer, are adopted to evaluate the proposed Markov chain model to determine RV under different environments. First, a peer with high trust performance results in high RV. We propose the average RV of analysis and simulation to evaluate the trust performance of peer in a group. The average RV of peer j performed in a group is defined as

$$\overline{RV}(j) = \frac{\sum_{n=1}^{N} RV_i^n(j)}{N}, \quad (1)$$

Where

$$RV_i^n(j) = \frac{\sum_{n=1}^{|R_g|} RV_i(j)}{|R_g|} \quad (2)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is the RV of peer j evaluated by peer i of the *n*th evaluation, and N is the number of computations. Higher the trust performance a peer executes, higher the average RV the peer generates.

Second, in this work a member with the highest RV of a group will be selected as the CA peer to authenticate and authorize group members. Therefore, we define the number of times a peer acted as a CA (i.e., denoted by NCA) or a backup CA (i.e., denoted by NBCA) to justify the trust performance of each peer. Higher the average RV a peer has, higher NCA the peer yields. The NCA and NBCA are defined as

$$NCA(j) = \sum_{n=1, if\ peer\ j\ is\ selected\ as\ the\ GL}^{N} 1 \quad (3)$$

$$\text{and}\quad NBCA(j) = \sum_{n=1, if\ peer\ j\ is\ selected\ as\ the\ backup\ GL}^{N} 1 \quad (4)$$

respectively. Where n is the *n*th evaluation.

3. REPUTATION ESTIMATION APPROACH

This section describes the Markov chain analysis-based RV estimation approach for the P2P network. The approach consists of two phases: the phase of Markov chain analysis model for determining RV, and the phase of CA management. This section depicts the first phase and next section details the second phase.

The Markov chain analysis model is used to determine the RV of each peer within a group. The first phase consists of three steps, including

Step 1: Creating the trust relationship among members,

Step 2: Defining trust events for transiting the trust state,

Step 3: Determining the RV of each member peer.

Step 1: Create the trust relationship among peers in group.

A peer's RV represents its trust manner performed in the group. A peer with good manners, such as Availability: available to share a file, to forward a query, to reply to a query. Contribution: a peer contributes positively to the system by uploading authentic files. Credibility/Honesty: Upon receiving a reputation query, a recommender peer sends an honest feedback. An example of peers' RV estimation after exchanging individual RV table among members is shown in Fig. 2. The group members include peers A, B, H, I, J and L.Each member is aware of 1-hop neighbor peers. The 1-hop neighbors of peer i is denoted by $N^1(i)$. For instance, node A's 1-hop neighbors, $N^1(A)$, are peer B, H and J. Peer B's RV evaluated by peer A is denoted by $RV_A(B)=2$.

Initially, each peer evaluates the trust manner of 1-hop neighbors, and then exchanges the trust manner information among 1-hop neighbors. Each peer then gathers its 1-hop neighbors' trust manner and stores the information in the RV relationship table, as indicated in Fig. 2. Next, a member averages other members' RV from the RV relationship table, and then stores the information at its local RV table. The averaged RV is formulated by

$$RV(i) = \frac{\sum_{j \in g} RV_j(i)}{|J|} \quad (5)$$

Where g is the group and |J| is the number of members.

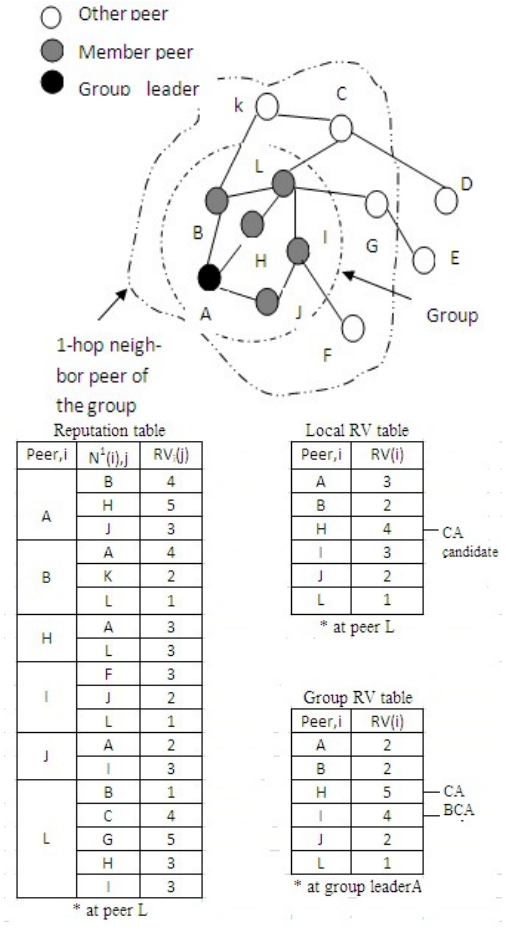


Fig.2. Reputation Value Estimation Process

After that, each peer determines the CA candidate from the local RV table and sends the table to the group leader. The group leader will obtain the group reputation value table by averaging each member's local reputation value table. The group leader then selects the member with the highest reputation value as the new CA peer and selects the member with the second highest RV as the new

Journal of Theoretical and Applied Information Technology
28th February 2013. Vol. 48 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BCA node. In the CA/BCA determination procedures, if there are several members with the same RV, they will compete based on the following three rules:

1) Priority 1: The member is current CA peer.
2) Priority 2: The member is current BCA peer.
3) Priority 3: The member's MAC address is the smallest one.

That the member first meets a higher priority rule will win the competition. For example, in the local trust table of peer L in Fig. 2, member H becomes the CA candidate because it has the highest reputation value. Member I becomes the BCA candidate because it has the second highest value and its MAC address is smaller than that of member A, as demonstrated in Fig. 2.

Step 2: Define trust events to transit trust state

A peer's reputation value changes according to its trust manner changes. For analyzing the steady state of each peer's reputation value, we assume that the change of trust state of each peer as a Markov chain model. Additionally, we define several events that will alter the trust state. A typical event table is shown in Table 1, in which good-manner events will increase the reputation value and bad-manner events will decrease the reputation value. Proposed trust events are classified into seven classes,which are shown in table 1.

Table:1 Event Table

Good manners	Reputation value	Bad manners	Reputation value
Normal leaving	+1	Abnormal leaving	-1
Normal joining	+1	abnormal joinjing	-1
Availability:available to share a file,to forward a query, to reply a query	+1	Unreliable:peer promise availability of specific services and do not deliver them	-1
Contribution: uploading authentic files	+1	Senders of inauthentic data	-1
Honesty:upon receiving a reputation query, a recommender peer sends an honest feedbank	+1	Liar peers: these peers lie in their feedbacks	-1
Win the BCA competition and it is not the current CA/BCA	+1	lose the BCA competition and it is not the current CA/BCA	-1
Win the CA competition and it is not the current CA	+2	lose the CA competition and it is not the current CA	-2

(1) Leave a group:

If a peer sends a LEAVE message to the group leader before leaving the group, this represents a normal leaving event and the reputation value of the leaving peer is thus incremented by one. Otherwise, the member's trust value will be decremented by one.

(2) Join a group:

If a non-member peer sends a JOIN message to request to a group normally rather than sending many JOIN messages in a short period, this represents a normal joining event. The reputation value of the joining node is thus incremented by one. Otherwise, the member's reputation value will be decremented by one.

(3) Availability:

peer availability - the extent to which a single peer contributes to the P2P service, based on the times at which it is online and willing to participate. workload availability - the average of the peer vail-abilities across all peers. This is often used as a coarse measure of the difficulty of hosting available P2P ser-vices on that peer set. service availability - the extent to which the P2P sys-tem is able to satisfy client requests. Because individ-ual peers, and so the resources they provide, are often unavailable, P2P systems typically employ some form of replication to achieve high service availability.[8]

(4)Contribution:

A peer contributes positively to the system up uploading authentic files or offering useful resources.

(5)Credibility/Honesty

Upon receiving a reputation query, a recommender peer sends an honest feedback.

(6) BCA competition:

If a peer wins the BCA competition and not the current BCA or CA, its reputation value will be incremented by one. On the other hand, if a BCA or CA node loses the BCA competition, its trust value will be decremented by one.

(7) CA competition:

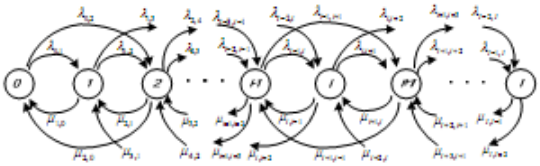
If a peer becomes the winner of CA competition and not the current CA, its reputation value will be incremented by two. Specifically, the CA peer manages the authority and authentication processes within a group. It should have the highest reputation value. If a CA peer loses the CA competition, its reputation value will be decremented by two.

Additionally, the state transition could be combined of different trust events. For example, a member's contribution is greater than the other member in a group. As a result, the peer reputation value will be incremented by three. In this work, only the defined trust events may change the trust state.

The trust events are lists in Table I. The state diagram of the trust events is shown in Fig. 3, which is the Markov chain model of the trust-state of the proposed approach with arrival rates of $\lambda_{i,i+1}$ and $\lambda_{i,i+2}$, and departure rates of $\mu_{i,i-1}$ and $\mu_{i,i-2}$ at state i, $0 \leq i \leq 1$. 0 is the lowest reputation value State 0 is the lowest trust state and I is the higest repuation value.

Journal of Theoretical and Applied Information Technology
28th February 2013. Vol. 48 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Step 3: Determine The Reputation Value Of Each Member Peer

We propose the Markov chain trust model to determine the probability of the steady trust-state for each member. This achieves two advantages:

1. to evaluate a member's reputation value based on its historical trust manner, which accurately determines member's trust and avoids malicious intrusions.
2. to determine the CA peer for each group, which solves the secure authentication and authority in a P2P network, and thus increases the P2P network s' security.

Theorem 1. The Markov chain trust model is an ergodic Continuous-Time Markov Chain, if it satisfies the required properties of the steady-state probability vector, i.e., time-homogeneous, irreducible and aperiodical.

The proposed trust model will be proven as an ergodic continuous-time Discrete-State Markov chain (namely CTMC) model. Consequently, the expected reputation value of each member can be determined after obtaining its unique steady-state probability vector.

Initially, a stochastic process of trust $\{X_t: t \in T\}$ is defined to establish a trust Continuous-Time Discrete-State Markov Chain model if for any time $t_i \in \mathbb{R}_0^+$, with $0=t_0<t_1 \ldots <t_n<t_{n+1}$, $\forall n \in N$, and the trust state $\forall s_i \in S=N$ for the probability mass function. Assume that the state sojourn time of the trust-events in the trust model is exponetially distributed, and thus has the following relation

$$P[Xt_{n+1}=s_{n+1}|Xt_n=s_n, \ldots, xt0=s_0] = P[Xt_{n+1}=s_{n+1}|Xt_n=s_n] \quad (6)$$

In other words, the proposed trust model has the memoryless property. This implies the current trust state only depends on the last trust state. Consequently, the trust model has the homogeneity property. The transition probability from state i to state j during the period [e,f) then can be expressed by

$$p_{ij}(e,f) = P[Xf=j|xe=i] \quad (7)$$

where, and $e,f \in T$ and $e \leqslant f$. The Chapman-Kolmogorov equation [9] for the transition probabilities of Eq. (7) of the trust CTMC is then derived by

$$p_{ij}(e,f) = \sum_{k \in S} p_{ik}(e,g) \square p_{kj}(g,f) \quad (8)$$

Where $0 \, e \leqslant g < f$.

Second, in Table I, the change of trust-states, $i \in S$, could be increased or decreased as the member's trust-manner is performed well or badly, respectively. Since the trust model considers both the member's trust-manner and CA/BCA competitions, all the trust states, $i \in S$ in the trust model can be reached from any other trust-states, $j \in S$, $j \neq i$. Any trust state is not an absorbing state, i.e., $p_{ij}=1$. This means the homogeneous model is irreducible and has the initial-state independent property, i.e.

$$\lim_{x \to \infty} p_{ij}(t) = \pi_j \quad (9)$$

Or

$$\lim_{x \to \infty} \pi_j(t) = \pi_j \quad (10)$$

Applying Eqs. (9-10) to Eq. (8), the state probability at time f is formulated as

$$\pi_i(f) = \sum_{i \in S} p_{ij}(e,f) \square \pi_j(e) \quad (11)$$

Therefore, the state probability vector, $\pi=[\pi_0, \pi_1, \ldots]$ at any instant time f can be expressed by

$$\pi_f = (\pi_e) \cdot P(e,f), \quad (12)$$

where P(e,f) is the transition probability matrix for any pair of trust states i and j at any time [e,f), $e, f \in T$ and $e \leqslant f$. The vector of the trust state probability is denoted by $\pi=[\pi_0, \pi_1, \ldots]$, in which the sum of the state probability is one,i.e., $\sum_j \pi_j = 1$.

Third, the member's trust state, i, is determined based on its trust-events: joining/leaving, availablity, Contribution, Credibility/honesty, CA/BCA competitions. Because the member's Contribution could be increased and decreased, and the competition-based trust-event breaks the periodical feature, the situations of these impact factors are changed aperiodically. Since a state i of the irreducible homogeneous trust CTMC model is aperiodical, the other states $j \in S$ are aperiodical. Consequently, all the trust-states of the trust CTMC model are all aperiodical. Based on the aperiodical transition among trust-states, the transition rate $q_{ij}(t)$ of the trust CTMC model from state i to state j is derived from the related the transition probability [10][11] as

$$q_{ij}(t) = \lim_{\Delta t \to 0} \frac{pij(t,t+\Delta t)}{\Delta t} \quad (13)$$

And

$$q_{ii}(t) = \lim_{\Delta t \to 0} \frac{pii(t,t+\Delta t)-1}{\Delta t} \quad (14)$$

Journal of Theoretical and Applied Information Technology
28th February 2013. Vol. 48 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where i ≠ j and $\sum_{j\in S} q_{ij}(t)=0$,∀i ∈ S,the infinitesimal generator matrix Q of the transition pr obaility matrix P= $[p_{ij}(0,t)]$= $[p_{ij}(t)]$ is defined as Q = $[q_{ij}]$. After applying Eq. (13) to Eq. (12) we have the differential equation

$$\frac{d\pi(t)}{dt}=\pi(t)\cdot P'(t)=\pi(t)\cdot Q(t), \quad (15)$$

Since the trust CTMC is time-homogeneous, we neglect the dependence upon time and then obtain

$$\frac{d\pi(t)}{dt}=\pi(t)\cdot Q \quad (16)$$

The steady trust-state probabilities are independent of time, and then we have $\lim_{t\to\infty}\frac{d\pi(t)}{dt}=0$ .As a result, the differential equation of Eq. (16) for solving the steady trust-state probabilities is simplified by the system of linear equations

$\pi\cdot Q=0$, (17)

and $\sum_j \pi_j=1$ (18)

The proposed trust model satisfies the required properties of the steady-state probability vector, i.e., time-homogeneous, irreducible and aperiodical. The theorem is thus proved. The result concludes the proposed model is an ergodiContinuous-Time Markov Chain, which can compute the trus steady-state probabilities, π_j, $j \in S$, for each member from
individual trust-manner.

4. NUMERICAL RESULTS

This section examines the proposed Markov chain analysis for the reputation value model by comparing the analytical results with the simulation results, analyzing the reputation values of peers, and evaluating the number of times a peer acted as a CA (namely NCA) or as a BCA (namely NBCA) of individual peer. Fig. 1 demonstrates the assumption for evaluations. several useful Parameter -s for analyses and simulations are given in table 2.
Initially, different incoming and departing rates for peer joining and leaving a group are adopted to evaluate the average reputation value and the speed of convergence of reputation value of each peer. The purpose is to verify that a peer with high trust performance generates a high reputation value, etc. Fig. 4 demonstrates the average reputation value of analytical and simulation of different trust performance under 30 peers. The average reputation values of analytical are very close to that of simulation even under low, middle, and high trust performances. However, some slight difference between analytical results and simulation results, for example, the average reputation values of peer 5 and 7 in the case of total number of peers is 30. Contributions of errors include event generations of the Poisson process and the Exponential distribution.

Table 2. Parameters For Analysis And Simulation

parameters	values
Number of peers	20-100
Number of group	3
Number of trust states	10
Arrive rate(possion distribution)	6-16
1-hop neighbour peers	20%
Peers' good behavior	random
Peers' bad behavior	random

Secondly, we examine the convergence of the analysis reputation value. Several factors, such as trust transition rate and values of trust state probability, may affect the speed of convergence of the analysis model. Fig. 5 shows the number of iterations required to converge of low, medium and high reputation values under different situation. Fig. 5 indicates that peers no matter with different trust classes or different initial reputation values, converge to their final trust values. Additionally, different trust classes result in the same speed of convergence, i.e., the speed of convergence is independent of the trust class under the same number of trust states. This is an excellent feature of the analysis model.

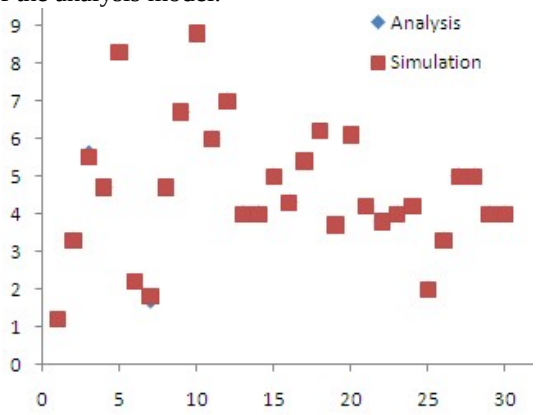


Fig.4. Analytical And Simulation Results Fo Different Trust Performance Of Peers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Finally, we examine the number of times a peer acted as a CA (namely NCA) and a BCA (namely NBCA), and the number of rejects (namely NREJ) by simulation. Results shows that the higher the average reputation value a peer has , the higher NCA and less NREJ the peer generates. Conversely, the lower the average reputation value a peer has, the higher NERJ and the less NCA reputation-value the peer yields. Moreover, a peer with medium reputation value generates higher NBCA but lower NCA and NREJ, a peer with high trust value yields high NCA and low NREJ, and vice versa.

5. CONCLUSIONS

This work proposed a two-step secure authentication for P2P network. First, the Markov chain analysis is adopted to analyze each one-hop neighbor's reputation value based on its previous trust performance. The analyzed reputation value is then
exchanged among all group members. The trust model is proved as an ergodic CTMC model. The node with the highest reputation value is then selected as CA that manages the group's reputation table. Numerical results indicate the analytical results are very close to the simulation results of light, medium, and high reputation values. The speed of the convergence of the analysis reputation value indicates the analyzed reputation value is independent of the initial values and trust classes.
This is a good feature for analytical models. Finally, the number of times a node acted as a CA and a BCA, and the number of rejects of a peer are examined. The results satisfy a peer with high reputation value yields high NCA and low NREJ, and vice versa.

6. ACKNOWLEGE

This work was supported by the Postgraduate Innovation Project Foundation of Jiangsu province (CXZZ11_0399) and the "qing and lan" project of nanjing university of posts and telecommunications(NY210045).

REFRENCES:

[1] He chaokai,Wu Meng, "Comparison and Analysis of Different Reputation Systems for Peer-to-Peer ", ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings, Chengdu, China, August 20-22, 2010, pp.320-323.

[2] R. Zhou and K. Hwang, "Gossip-based reputation aggregation for unstructured peer-to-peer networks," in Proceedings of IEEE Interational Conference Parallel and Distributed Processing Symposium, 2007, pp. 1-10.

[3] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing" IEEE Trans. Parallel and Distributed Systems., vol. 18, noA ,2006, ppA60-473.

[4] D. Kamvar, M. Schlosser, and H. Garcis-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," Proc. Word Wide Web Conf(WWW2003), ACM Press, 2003, pp. 640-651.

[5] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no.7, 2004, pp.843-857.

[6] eBay. eBay home page, http://www.ebay.com. 2009.

[7] Tbao. Tbao home page, http://www.taobao.com

[8] Richard J. Dunn, John Zahorjan, Steven D. Gribble, Henry M. Levy," Presence-Based Availability and P2P Systems," Fifth IEEE International Conference on Peer-to-Peer Computing, P2P 2005, v 2005, p 209-216, 2005

[9] G.D. Hachtel, E. Macii, A. Pardo and F. Somenzi, "Markovian Analysis of Large Finite State Machines," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 15, Issue 12, pp. 1479-1493, Dec. 1993.

[10] L. Kleinrock, Queueing Systems Volumn 1: Theory, Wiley-Interscience, 1975.

[11] Ben-Jyeyu Chang,Szu-Liang Kuo, Ying-Hsin Liang,De-Yu Wang, "Markov Chain-based Trust Model for Trust Value Analysis and Key Management in Drstributed MANETS" IEEE Transcation on vehicular technology, Vol. 58, No.4, pp.1486-1863, May 2009.