Construction of Trust Based Dynamic Access Control Model in P2P Network Environment

Yingjun Han, Xiaojie Cui
North China University of Science and Technology
Tangshan, Hebei, 063009, China
yjhanh@163com

Journal of Digital Information Management

ABSTRACT: *With the development of society and technology, sharing of resources has become an indispensable component in our life. With its congenital features of high speed, rich resources, strong fault-tolerance and low cost, peer-to-peer (P2P) network occupies an important status in network resources sharing. However, this technology has serious problems in network security, especially in trust management and access control. Therefore, based on the advantage of trust management and Role based access control (RBAC), this study proposed a trust based dynamic access control model in P2P network environment, which allocates general roles by automated trust negotiation, to build dynamic trust relation among strange entities, then the internet calculates users' trust in real time. General role whose trust is over threshold derives a series of temporary roles with privilege limit set which can access network resources and thus realize the dynamic authorization policy for small control granularity.*

Subject Categories and Descriptors
I.6.4 [Model Validation and Analysis]: RBAC Model; **G.2 [Discrete Mathematics]**

General Terms: Peer-to-Peer, RBAC Mode

Keywords: Peer-to-Peer, Trust, Access Control, Role Based Access Control Model

Received: 18 February 2016, Revised 19 March 2016, Accepted 24 March 2016

1. Introduction

P2P (Peer-to-Peer), a burgeoning distributed network model, has been extensively applied in fields of distributed computation, file sharing, electronic commercial, etc[1,2]. However, most works targeting on P2P technology concentrates on aspects such as resource location, message routing, parallel downloading, etc., while how to set access control policy for sensitive resources in the network is seldom researched. Access control, a main method for restricting users to access to systematic resources without permission, can provide security guarantee for system [3]. The existing access control model aiming at distributed application is usually set for C/S architecture (client/server architecture), which assumes that there is an authoritative center in the system to carry out the pre-determined access control policy, and to grant access privilege according to identity of request entity [4]. Such a model is actually a centralized management model, which only suits for closed system, and its visiting strategy can only identify familiar user but cannot effectively process new user.

Role based access control (RBAC) is a common type of traditional access control, which, by introducing a concept of role to realize the separation of user and authority, reduces the cost of authority management, and supports authorization constraint in a better way[5,6]. However, in P2P environment, there are too many unfamiliar users, thus the owner of resources is hard to grant privilege based on identity of strangers, hence it is difficult for traditional RBAC to apply to this situation. Based on this, this paper, combining the advantage of trust management system and RBAC policy, re-calculates trust of trust evaluation indexes and re-defines the essential elements in the model in order to construct a dynamic access control model in P2P network environment.

2. Theory and Background

2.1 Basic concepts of trust

Trust is a subjective conception, which can be recognized

as the degree of subjective probability of one entity to evaluate other entities. The evaluation is performed before its monitoring of such behavior and in the situation where the behavior has certain influence on its own behavior. It is an important aspect in people's life. People deal with social affairs like interpersonal interaction depending on trust. And trust is widely studied in areas of sociology, psychology, philosophy, etc. [7,8].

Computer network actually acts as a miniature of the human society; however, unreal network environment blocks the establishment and maintenance of trust relationship, which generates multiple security issues. With the development of technology, the existing security technology allows the initial establishment of trust. For example, encryption algorithm provides privacy protection and digital signature, authentication protocol provides authorization of authentication and access control, meanwhile, PU comes into being as a trust management system. But traditional trust management protocol based on QS structure doesn't apply to P2P network. Therefore, trust management protocol suitable for P2P safety issue remains to be discussed.

2.2 Trust evaluation

In this paper, we introduce the concept of Trust for trust evaluation of the model:

Trust is a quantitative description of the degree of one entity's trust in another entity. In many studies, trust is described as a real interval, e.g., [0, 1], 0 for Do Not Trust, 1 for Full Confidence. Compared to general probability model, such kind of model is characterized by uncertainty, which is mainly based on such a consideration: when one entity knows nothing at all of another entity, we cannot simply describe such a state using Trust or Do Not Trust. The introduction of uncertainty effectively solves this problem.

2.3 Access control technology

Access control system restricts the access to key resources, preventing illegal users' entering the system and legal users' illegal using of the resources. Existing main access control technology includes: discretionary access control (DAC), mandatory access control (MAC) and role based access control (RBAC) [9].

DAC and MAC is mainly for granting privilege for personal user. Users visiting large-scale system is usually diverse in category, huge in amount and changeable, leading to high risks of error. Role based access control (RBAC) which comes into being in recent years connects role introduced with privilege, grants privilege to users by allocating appropriate roles, and realizes the logic separation of user and access privilege. In this way, authorization has much stronger operability and manageability compared with individual authorization, thus is very suitable for authorization management of large-scale user management information system.

3.Calculation of Trust

Global trust mode based in social trust network put forward recently aims at solving fraudulent conduct and unreliable service. In trust model, node has a unique trust value, which integrates trust evaluation of this node in the whole network, thus is comprehensive and accurate. Based on previous studies [10-12], this paper generates a mathematic description of the global trust model:

$$s_{ij} = sat_{ij} - unsat_{ij}, r_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)}, t_i^{(k+1)} = (1-\alpha) p_i + \alpha \sum_{j=1}^{n} (r_{ij} t_j^{(k)}) \quad (1)$$

Herein two-tuples<sat_{ij}, $unsat_{ij}$> means success and failure times of interaction of node i and node j, s_{ij} means local trust of node i to node j, and local trust obtained after s_{ij} being standardized, which is described as r_{ij} j . t_i means global trust of node i. α is the invariant of interval$(0,1)$. p_i is the default probability distribution, whose calculation method is as follows: Assuming that there's a high trust node set H, H is composed of moderator and early users in EigenTrust model, and in PowerTrust model, H is composed of Power node set elected dynamically by the system. When $p_i \in H$, $p_i = 1/m$; or $p_i = 0$; m means the number of nodes in set H.

It is pointed out by recent studies that, some nodes in P2P system possess congenital privileges due to the existence of high trust node, which is similar with reliable third party in the network, while P2P network rejects this protocol. Therefore, they proposed a global trust model which solves global trust value of node by constructing linear equation set conforming to iterative convergence and that model is absence of high trust node set. However, without H, linear equations become homogeneous linear equations. According to knowledge of linear algebra, when coefficient matrix is with full rank, the solution of homogeneous linear equations is null vector; when coefficient matrix is non-full rank, homogeneous linear equations has multiple solutions, while global trust value of node has to be unique non-null vector. Thus this method doesn't apply to the solution of node's global trust value in P2P network. In view of the above-mentioned shortcomings, based on PageRank algorithm, this paper puts forward a calculating model of global trust value without need of high trust node set:

$$s_{ij} = q(1 - \exp(-sat_{ij}))\exp(-unsat_{ij}) + \varepsilon. \quad (2)$$

$$r_{ij} = w \cdot \frac{s_{ij}}{\sum_{j=1}^{n} s_{ij}} + (1-w) \cdot \frac{1}{n} \quad (3)$$

$$t_i^{(k+1)} = \sum_{j=1}^{n} (r_{ji} t_j^{k}) \quad (4)$$

Herein, $exp(x) = e^x$ is exponential function; q is magnification factor, which can be any larger value, here set as $q = 1000$; n is total number of nodes in network; ε is a very small value, which can be set as $\varepsilon = 10^{-5}$; w is weighted factor, usually is set as $w = 0.9$, i.e., node i has a 90% credibility of trust built through interaction history, while when there's no interaction history, node i can only give a mean trust to each node, of which the credibility weight is set as 10% by the system.

Set matrix as $R = (r_{ij})$. According to equation (2) and (3), we know that matrix R is row random matrix, which can be used as transition probability matrix of Markov chain of finite state, whose state set is all the nodes in the network. In the Eigentrust and PowerTrust model, the existence of high trust node set not only accelerates iterative convergence, but also guarantees aperiodicity and irreducibility of Markov chain in finite state. In the model of this paper, these two features are guaranteed by the nature of local trust r_{ij}. According to equation (2) and (3), in Markov chain's transition probability matrix R, there is no any absorbing state, and each state has a transition probability to other states; vice versa. Meanwhile, each state has its self transition probability. According to lemma 1.1 and 1.2 in literature [13], Markov chain corresponding to transition probability matrix R in finite state has irreducibility and aperiodicity. Thus this Markov chain is traversable, and there must be a unique stationary distribution. Set stationary distribution as vector $\vec{t}$, which must conform to: $\vec{t} = R^T \times \vec{t}$. The above-mentioned stationary distribution obtained iterative repetition is the principle eigen vector of matrix R^T(eigen value λ=1). This stationary distribution is the limit probability distribution of Markov chain corresponding to the transition probability matrix R. Therefore, the iteration of equation (4) is convergent, which has nothing to do with default value of vector $\vec{t}$, and default value is usually set as uniform distribution. Vector $\vec{t}$ obtained after iterative convergence is the global trust of all nodes what we want to solve.

4. Trust Based Dynamic Access Control Model (TBDAC)

4.1 Essential elements of the model

The model of this paper is obtained by extending trust and temporary roles based on RBAC model, and is composed of the following parts, i.e., user U, general role R, temporary role TR, trust T and privilege P. User and role will not be bounded together; user and role server abide by automated trust negotiation, which allocates general role set to users. When user accesses internet, network will calculate its trust value, then the temporary role derived by general role will be activated, and user will getcertain access privilege.

Definition 1: Model TBDAC ={USERS, ROLES, TDRS, PERMS, TRUSTS}, of which USERS, ROLES, TRS, PERMS and TRUSTS means user set, role set, temporary role set, privilege set, and trust set, respectively.

Definition 2: Basic relation of Model TBDAC

$UA \subseteq USERS \times ROLES$, means that each role is allocated with a set of roles;

$PA \subseteq PERMS \times ROLES$, means that each role is allocated with a set of privilege;

$RR \subseteq ROLES \times ROLES$, means the inherition relationship between roles, PR is partial ordering relation, marked as $\leq$, if $r_1 \leq r_2$, then r_2 covers all the privileges of r_1;

$PP \subseteq PERMS \times PERMS$, means the inherition relationship between privileges, PP is partial ordering relation, marked as $\leq$, if $P_1 \leq P_2$, then P_2 covers all the privileges of P_1.

4.2 User/role allocation based on trust negotiation

In P2P environment, RBAC model cannot effectively promote the set up of trust relationship between two parties due to the large amount of network user and unlimited entrance and exit, leading to difficulty in completing role allocation task. On account of that, we formulated role allocation mechanism referring to automatic trust negotiation. Role server declares role allocation strategy; users can access to network resource only when corresponding trust certificate is prepared according to the role allocation strategy.

Definition 3: Trust certificate is a digital certificate of privilege attribute issued by authoritative institution, including signature of the issuing institution, public key of trust certificate holder and so on, to allocate roles for users, marked by C, and Credential is for certificate set. For example, X.509V3 expanding certificate, and RT trust certificate, etc.

Definition 4: Role-allocation strategy stipulates the trust set necessary for obtaining roles, markd by P.
Role-allocation format is described as:

$$p(r \leftarrow (c_{11} \wedge c_{12} \wedge .... c_{1k}) \vee ..... \vee (c_{l1} \wedge c_{l2} \; .... c_{ln}))$$

Which means that:

$$(own(u,c_{11}) \wedge ... \wedge own(u,c_{1k}) \vee ... \vee (own(u,c_{l1}) \wedge ... own(u,c_{ln})) \Rightarrow \{accept, reject\}$$

Herein function own: USERS × Credential '! {true,false} judges if a user has certain certificate. l, n, k are nature natural number; $p(r \leftarrow (c_{11} \wedge c_{12} \wedge \cdots \wedge c_{1k}) \vee \cdots \vee (c_{l1} \wedge c_{l2} \wedge \cdots \wedge c_{ln}))$ is the clause of Policy P.

4.3 Role/privilege allocation based on trust

In the above-mentioned role allocation process, trust certificate disclosed to role server by user is long-term effective, and role obtained by this is called general role, which cannot be activated directly. That is because trust of users and network resources changes with time and the context, and changes of trust can directly affect use of user privilege. To apply to dynamic network environment,

this paper derives a series of temporary roles from general roles. When user needs to perform a task, at first network will calculate user's trust, only when the value is over the activation trust threshold, can temporary roles be activated, and get corresponding access privilege. Besides, changes of user's trust will reflect the change of its access privilege.

Definition 5: Temporary role TR is derived by general roles, with a nature of timeliness. TRS $\subseteq$ ROLES × PERMS ×TRUST means the correlation of temporary role sets with privilege set and trust set.

$$TRS=\{r_1,r_2,..r_m,<p_1,t_1>,<p_2,t_2>,...,<p_n,t_n>|r\in ROLES,p\in PERMS,t\in TRUST\}$$

Herein m, n are natural number.

Definition: relation of temporary roles are partial ordering relation, set < R, $\leqslant_1$ >, < P,$\leqslant_2$ > and < T,$\leqslant_3$ > as partial ordering sets, then define relation $\leqslant_4$ on the basis of set R × P×T as follows;

$\forall$ < r_1, p_1, t_1 >, < r_2, p_2, t_2 >$\in$R × P ×T, < r_1, p_1, t_1>$\leqslant_4$< r_2, p_2, t_2> when and only when $r_1\leqslant_1 r_{2,}$ $p_1\leqslant_2 p_2$, $t_1\leqslant_3 t_{2,}$ then < R × P × T, $\leqslant_4$ > is a partial ordering set.

Testify: Only need to prove that $\leqslant_4$ has reflectivity, ant symmetry and transitivity.

First, testify $\leqslant_4$ has reflectivity:
$\forall$< r, p, t > $\subseteq$ R × P × T, then r □ R, p □ P, t □ T, and because < R, $\leqslant_1$>, < P,$\leqslant_2$> and < T,$\leqslant_3$ > are partial ordering sets, partial relation $\leqslant_1$, $\leqslant_2$,$\leqslant_3$ have reflectivity, then r $\leqslant_1$r,p $\leqslant_2$p,t $\leqslant_3$t, that is < r, p, t> $\leqslant_4$< r, p, t>, so $\leqslant_4$ has reflectivity.

Second, testify $\leqslant_4$ has antisymmetry:
$\forall$< r_1, p_1, t_1>, < r_2, $p_{2,t2}$ >$\in$ R × P × T. If < r_1, p_1, t_1 >$\leqslant_4$ < r_2, p_2, t_2 >, < r_2, p_2, t_2 > < < r_1, p_1, t1>, then $r_1\leqslant_1 r_2$, $p_1\leqslant_2 p_2$, $t_1<_3 t_2$, $r_2\leqslant_1 r_1$, $p_2\leqslant_2 p_1$, $t_2\leqslant_3 t_{1.}$

Because < R, $\leqslant_1$ >, < P, $\leqslant_2$ > and < T, $\leqslant_3$ > are partial ordering sets, so partial relation $\leqslant_1$, $\leqslant_2$, $\leqslant_3$ have antisymmetry; Because $r_1<_1 r_{2,}$ $p_1\leqslant_2 p_2$, $t_1<_3 t_2$ and $r_2\leqslant_1 r_1$, $p_2\leqslant_2 p_1$, t2$\leqslant_3$ t_1 then $r_1 = r_2$, $p_1 = p_2$, $t_1 = t_{2.}$ So < r_1, p_1, t_1 >=< r_2, p_2, t_2>, then $\leqslant_4$ has antisymmetry.

Third, testify $\leqslant_4$ has transitivity:
$\forall$< r_1, p_1, t_1 >, < r_2, p_2, t_2 >, < r_3, p_3, t3 > $\in$ R × P × T, if < r_1, p_1, t_1 >$\leqslant_4$ < r_2, p_2, t_2> and < r_2, p_2, t_2 >$\leqslant_4$ <r_3, p_3, t3>, then $r_1<_1 r_2$, $p_1\leqslant_2 p_2$, $t_1\leqslant_3 t_2$, $r_2\leqslant_1 r_3$, $p_2\leqslant_2 p_3$, $t_2\leqslant_3 t_{3.}$ And because $<_1$, $<_2$, $<_3$ have transitivity, so $r_1\leqslant_1 r_3$, $p_1\leqslant_2 p_3$, $t_1\leqslant_3 t_{3,\ so}$ < r_1, p_1, t_1 > $\leqslant_4$ < r_3, p_3, t_3>, so $\leqslant_4$ has transitivity.

According to the above three steps, we can know < R × P × T,$\leqslant_4$> constructs a partial ordering set,relation of temporary roles is partial relation.

Definition 6: Privilege of temporary role is the actual privilege of its activation, marked as RA(r). It is a subset of the pre-determined general role privilege PA(r), i.e., RA(r)$\subseteq$ PA(r). RA(r) is determined by pre-determined general role privilege and trust threshold established in the policy, $PA(r_i) \wedge t_i \rightarrow_{RA(r)}$

RA(r), i.e., $RA(r)=\{< p_1,t_1>,\cdots< p_n,t_n>\}$

Definition 7: RA $\subseteq$ TRS × PERMS × TRUSTS means temporary role/privilege allocation with trust threshold. Set (r, p, t) $\in$ RA, then an user with temporary role r obtained from t ' (t'$\geq$ t) can exercise privilege P.

Correlating the trust threshold reflecting privilege sensitivity to the allocation policy of temporary role/ privilege is actually adding constraint to privilege, thus only user with role obtained from t ' (t'$\geq$ t) can have access privilege, and this promotes the keeping users' good credit and healthy development of the network.

Definition 8: Function ActivedTRoles(r:$\rightarrow$TDRS) TRUSTS means the activated trust threshold of temporary role r. TRUSTS is the minimum trust needed for user to activate its temporary role, which equals the minimum trust threshold allocated to privilege of temporary role: ActivedTRoles(r) = min({t| $\subseteq$ p: PERMS $\vee$ (r, p, t) $\subseteq$ RA).

5. Conclusion

This study proposes a dynamic network access control model based on trust by combining the advantages of trust management and RBAC model. The mode can determine the category of tole and dynamically confirm whether it has visit privilege by calculating trust of user, which can effectively restrain unsafe visit and protect safety of user resource in P2P environment. It overcomes the shortcomings of traditional RBAC model has improved sensitivity to distinguish privilege, thus realize fine-grained authorization.

References

[1] Liang, Wang., Yajun, Guo., Mei, Qi (2009). A Reputation-Based Trust Evaluation Model for P2PE-Commerce. *Distributed Sensor Networks*, 5 (39) 39-44.

[2] Zaiping, Suo., Lijun, Guo., Xiaofeng, Zhang (2010). Client software system based on C/S mode. Computer and Information Technology,14. 89-91.

[3] Meng, Xingu., Ding, Yalin., Gong, Yue (2012).Trust: A trust model based on feedback-arbitration in structured P2P network. *Computer Communications,* 25 (4) 357-364.

[4] Taddeo, Mariarosaria., Vaccaro, Antonino (2011).Analyzing Peer-to-Peer Technology Using Information Ethics. *Information Society,* 27 (2) 105-112.

[5] Pouwelse, J.A., Garbacki, P. , Wang, J. (2007). Tribler: A social-based peer-to-peer system. *Concurrency and Computation,* 19 (1) 1-11.

[6] Wen, Dou., Minhuai, Wang., Yan, Jia(2004). A Recommendation-Based Peer-to-Peer Trust Model. *Journal of Software,* 15 (4) 571-583.

[7] Sandhu, R S., Coyne, E J., Feinstein, H L., Youman, C E. (1996). Role-Based access control models. *IEEE Computer*, 9 (2) 38-47.

[8] Zhou, R., Hwang, K. (2007). PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Transactions on Parallel and Distributed Systems,* 18 (5) 460-473.

[9] Jianli, Hu., Bin, Zhou., Quanyuan, Wu (2011). Researchon incentive mechanism integrated trust management for P2P networks. *Journal on Communications,* 32 (5) 22-32.

[10] Bravoa, Giangiacomo., Squazzonib, Flaminio., Boeroc, Riccardo (2012). Trust and partner selection in social networks: An experimentally grounded model. *Social Networks,* 14 (7)13-25.

[11]Taddeo, Mariarosaria., Vaccaro, Antonino (2011). Analyzing Peer-to-Peer Technology Using Information Ethics. *Information Society*, 27 (2) 105-112.

[12] Chunbin, Zhang., Xiaohua, Qin., Yucui, Guo (2012). A reputation-based trust management model in P2P network. *Computer Era*, (3) 17-19.

[13] Jintao, Li., Yinan, Jing., Xiaochun, Xiao (2007). A Trust Model Based on Similarity-Weighted Recommendation for P2P Environments. *Journal of Software,*18 (1) 157-167.

.