Trust-Based Service Matching Access Control Model

Zhang Yongsheng
School of Information Science and Engineering, Shandong Normal University
Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology
Ji'nan 250014, China, 15666965768
zhangys@sdnu.edu.cn

Li Yuanyuan
School of Information Science and Engineering, Shandong Normal University
Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology
Ji'nan 250014, China, 18954162974
lizzy.01@163.com

Wu Mingfeng
School of Information Science and Engineering, Shandong Normal University
Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology
Ji'nan 250014, China

***Abstract*—By the research of Web service architecture, the article puts forward a new trust-based access control model, which is based on service-oriented architecture (SOA) and combines with service matching. The model puts the trust as matching criterion. Transaction is divided into three grades according to the level of trust. The different requests are matched appropriate services. That balances the network load, and improves resource utilization. In the model, LRU algorithm is used for the replacement of service to improve the efficiency of the system. The article proposes a new trust calculation method, exponential smoothing is used for trust forecast, to further ensure the safety of service computing.**

Key words-access; control; matching; trust; exponential smoothing; M-TBAC

I. INTRODUCTION

Web service[1] is an application with the feature of self-contained and self-describing, it can publish, query and call through web, user can integrate web service online into own application to complete the task without duplication of development, web service provides a mode, which is language-independent, and data can be shared between machine and machine in the mode[2].

Paper [3] proposed the concept of trust management, which covers some of the traditional access control models, such as access control matrix, access control lists ACL [4]. Whether it is based on probability or the average, there are a variety of trust degree calculation method, which all use the two-dimensional computing model. For example, paper [5] proposed WS-TBAC model, the calculation of trust uses regret system algorithm, direct trust and recommended trust are respectively called individual latitude and society latitude, the calculation of individual latitude is according to setting different weights of events, if recommenders provided false recommendation, took appropriate punishment mechanism, but not fundamentally avoid false recommendation[6,7].

To solve the above problem, the paper introduces a trust mechanism.The rest of this paper is organized as follows. Section II outlines description and update of service, followed by the calculation of trust and trust forecast in Section III. Section IV gives the trust-based service matching access control model. The experiment is introduced in Section V. Finally, Section VI concludes the paper.

Natural Science Foundation of Shandong Province of China under Grant No. ZR2011FM019；Postgraduate Education Innovation Projects of Shandong Province of China under Grant No. 292.

II. DESCRIPTION AND UPDATE OF SERVICE

A. Description of Service

Storage node contains three parts: Serial ID (express request or service type with Arabic numerals); Important Coefficient IC (the higher value of trust, the greater value of IC); Pointer domain next. Request and service nodes structure as shown below:

Figure 1. Description of request and service nodes

ID=1,2,3,⋯,m(m is a positive integer); IC=n∈[1,2,3], IC is 1,general affairs; IC is 2, more important affairs; IC is 3, the most important affairs.

B. The Insertion of Service

Assuming that the system in the R, S tables as shown below:

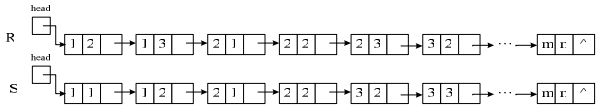


Figure 2. Requests and services linked list storage structure

Assuming that there is a request, whose ID is 3,IC is 1;there is a service, whose ID is 1,IC is 3.The nodes are shown below:

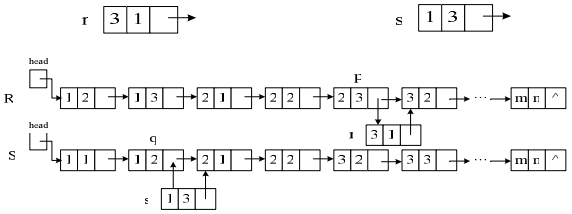


Figure 3. The insertion of nodes

Insertion code is as follows:

```
//rs is a collection of R, S- list , Node is node object
    public void insertNode(Node n)
    {       foreach(Node x in rs)
            {       if(x.ID == n.ID)
                    {   if(x.IC + 1 == n.IC)
                        {   rs.add(rs.indexOf(x)+1, n);
                                    }
                    }
                        else if(x.ID + 1 == n.ID )
                      {  rs.add(rs.indexOf(x)+1, n);}
    }
```

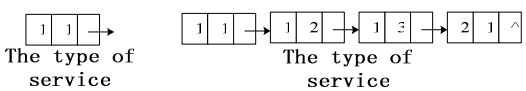
III. SERVICE MATCHING STRATEGY

In a cycle, each service and request all have ID and IC.

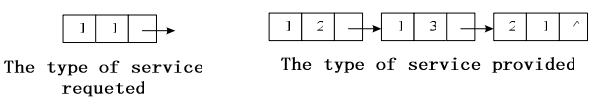
First, the ID of request and service must be the same, which is a matching service must be the service needed by the requester.

Second, when service and request's ID is the same, select service's IC bigger or equal to request's IC to match, and select eligible service whose IC is the biggest.

For example: Request's ID is 1,IC is 1; the types of services contain: ID=1， IC=1； ID=1， IC=2； ID=1， IC=3；ID=2，IC=1.



Now, should match the service whose ID is 1and IC is1. However, services provided are as follows:



Now, should select service whose ID is1 and IC is 2.Although the trust of service whose ID is 1and IC is 3 is bigger and better, the service whose IC is 2 has met the need, the service of which IC is 3 is ready for higher expectations. Service matching code is as follows:

```
for(int i=1;i<R.length;i++)
{   for(int j=1;j<S.length;j++)
        { if(r.ID==s.ID)
          { if(r.IC<=s.IC)
            return s;}
          else s=s->next;}
    r=r->next;
}
```

IV. THE CALCULATION OF TRUST AND TRUST FORECAST

A. *The Calculayion of Trust*

1) Direct View(DV)

DV is trust calculation method by direct interaction, subject makes trust evaluation to object according to direct interaction experience. The value of DV is decided by two aspects: history of direct interaction, the service requester's own security configuration [8].The formula of requester's history trust h_{rp} is:

$$h_{rp} = \frac{s(r,p)}{s(r,p) + \sum_{k=1}^{f(r,p)} \rho_k \left(\frac{T_h}{T}\right)} \qquad (1)$$

Service requester is described r, service provider is described p; $s(r,p)$ and $f(r,p)$ are respectively the times of success and failure; ρ_k is the punishment coefficient on the failure behavior, $\rho_k = e^{(T_h/T)}$, T_h is trust threshold, T is comprehensive trust; Initially, the requester r does not have interactive behavior, $h_{rp} = 0$， $h_{rp} \in [0,1]$， the more times of interaction, the more trusted for requester, h_{rp} tends to 1,and vice versa.

The formula that security configuration e_p of service requester is:

$$e_p = \sum_{x=1}^{n} C_x(r,p) \qquad (2)$$

x is a security need of service requester, assuming that service requester have n security needs; $C_x(r,p)$ is the weight after meet a security need. If not meet this security need, the value of $C_x(r,p)$ is 0, $C_x(r,p) \in [0,1]$.

Security needs and weights are shown in table Ⅰ:

TABLE Ⅰ SECURITY NEEDS AND WEIGHTS [8]

Security needs	**Instruction**	$C_x(r,p)$
Verification TPM	Equipped with TPM or not	0.3
Encrypt communication channel	communication channel is safe or not	0.1
Platform remote attestation	Platform environment authentication	0.4
Platform access control	Platform access control verification	0.2

The formula of DV is:

$$\begin{aligned} DV &= \alpha h_{rp} + (1-\alpha) e_p \\ &= \alpha \frac{s(r,p)}{s(r,p) + \sum_{k=1}^{f(r,p)} \rho_k \left(\frac{T_h}{T}\right)} + (1-\alpha) \sum_{x=1}^{n} C_x(r,p) \end{aligned} \qquad (3)$$

$\alpha \in [0,1]$, the formula (3) is conventional subject security state assessment, without regard to its historical behavior.

2) Recommendation View (RV)

RV is trust evaluation which subject combines recommended information and recommender itself to make trust evaluation for object [9].

$$RV = \frac{\sum_{p \in P} \sum_{m=1}^{k_r} \frac{T_m(r, p, t)}{\varphi}}{\sum_{p \in P} k_r} \quad (4)$$

P stands for a object collection which has ever interacted with requester r, Tm（r, p, t）is trust in m time between requester r and provider p.

φ is penalty coefficient, when the interaction is successful, φ is 1; when the interaction is unsuccessful, φ is bigger than 1. When the two sides do not have interaction history, RV is initialized to 0.

3) Public view (PV)

PV is a public opinion, select five individuals who have good performance in recent period as a monitoring group.

$$PV = \sum_{m=1}^{5} V_m(r, p) \quad (5)$$

$V_m(r, p)$ is public view of r from monitoring group, PV is weight sum of 5 public views.

4) Comprehensive trust (T)

T is weight sum of three trust view.

$$T = \omega DV + \eta RV + \mu PV \quad (6)$$

$\omega + \eta + \mu = 1$, direct view the results of interaction between the current object P and the subject r, trust reflected by direct view is more important than recommendation view. Therefore, under normal circumstances: $\omega > \eta$

B. Trust Forecast

In view of the fact the trust changes with time and the environment of the surrounding network [10]. People want to generate the historical sequence of credibility to predict the future credibility of value, so that the credibility of value for the user to interact.

Exponential smoothing method is used to make a smooth function of predicting smoothed values [11], using small errors between smoothed value TS and actual value TA to update the next TS value. T_{t-1}^{A} is the trust value after the time t-1 interaction, and T_{t-1}^{S} is the smoothed value in the period of t-1. By $(T_{t-1}^{A} - T_{t-1}^{S})$ got from step t multiplies a scale factor to fix the smoothed value of t-1, and obtain the smoothed value of the time t.

The formula of smoothing trust value is as follows:

$$T_t^S = T_{t-1}^S + \alpha(T_{t-1}^A - T_{t-1}^S) \quad (7)$$

In the above formula, α is smoothing constant，$0 < \alpha \le 1$。

By collation, get the exponential smoothing formula:

$$T_t^S = \alpha T_{t-1}^A + (1-\alpha) T_{t-1}^S \quad (8)$$

$0 < \alpha \le 1$（t≥3）。

By setting $T_2^S = T_t^A$ or $T_2^S = \frac{1}{3}\sum_{t=1}^{3} T_t^A$ to initialize calculation process. At the same time, because exist once interaction, $T_1^A \ge 0$.

Get from the formula (8):

① The bigger of the value of α ,the faster changes in the smoothed values, and vice versa.

② When getting smoothing value, the weights of older decay quickly.

The equation is as follows from the above:

$$T_t^S = \alpha \sum_{j=1}^{t-1} (1-\alpha)^{j-1} T_{t-(j-1)}^A + (1-\alpha)^{t-2} T_2^S, t \ge 2 \quad (9)$$

$$T_1^A \ge 0$$

In the above formula, the weight of T_{t-1}^A is：

$$W_{t-1} = \alpha(1-\alpha)^{t-1}$$

③The value of α is got from trial and error or minimizing the MSE.

④ Using $T_{t+j}^S = \alpha T_{t-1}^A + (1-\alpha) T_{t+j-1}^S$ to predict values after the point of t-1（T_{t-1} is the last point which has actual credibility）

V. THE CALCULATION OF TRUST AND TRUST FDRECAST

Summarizing the above analysis, this paper presents Trust-based Service Matchmaking Access Control Model in the service computing environment (M-TBAC). The model is shown in Figure 4.

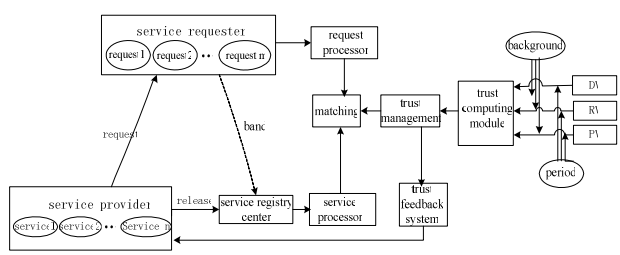


Figure 4. Trust-based Web Service Matching Access Control Model

Service provider uses Service Profile structure to describe service (service discovery) and safety strategy needs. Service provider releases the feature of services to service registry center. And then send services released to service processor to making future services processing.

Service requester puts forward service requests, and send requests (including service type, function, security strategy, etc.) to service processor, and in accordance with the requested information to create request service template and use the framework of the Service Profile describes it out.

Service and profile instance needed by security strategy are released in service registry center, services requested by requester and profile instance needed by security strategy are at the side of requester. Then, match request and service by match maker, and service discovery [12].

Trust computing module is used for computing of trust, combining with background and period of interaction, using DV, RV and PV. Then send the result to trust management system. On the one hand, trust management system sends trust results to match maker to assist the service matching; On the other hand, feedback results to trust feedback system, then pass to service provider, record the performance of the service requester to prepare for the follow-up query.

VI. SIMULATION EXPERIMENT RESULTS AND ANALYSIS

In order to test the performance of models, use Java to design and implement the prototype system (Semantic Web Services Discovery and Rank System, SWDRS）.

The main purpose of the experiment is to test the congestion degree of model, so need to test the model's performance under different load. Set number of business flow, respectively 4, 6, 8, 10, 12, 14, means the number of service request. The more business flows are, the heavier the load in the network.

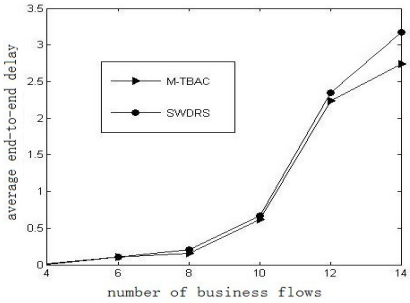


Figure 5. Average end-to-end delay of the two models under different load

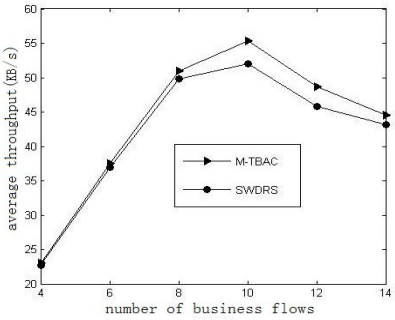


Figure 6. Average throughout of the two models under different load

Seen from Figure 5, 6, when the number of business flows are 4 and 6, almost do not appear congestion, the model and SWDRS system performance curve is almost consistent. With the load increasing, this model has better performance than the SWDRS system. This is why matching principle of M-TBAC model is based on the original semantic matching, under the premise of meeting needs, select the service having minimum integrated trust. Rather than talk to other demanding the requester competition. This allows more requests to be met within the shortest possible time.

VII. CONCLUSION

This paper presents trust-based services computing access control model which puts service matching as the main basis, select services needed depending on different trust requirements. To some extent, ease the problem that majority of users waiting for the same high-grade service, reduced the probability of network congestion. Give trust prediction method using exponential smoothing, which is better able to adapt to the dynamic changes of service computing environment, further ensuring the security of the network .

ACKNOWLEDGMENT

This research was supported by Natural Science Foundation of Shandong Province of China under Grant No. ZR2011FM019. It was also supported by Postgraduate Education Innovation Projects of Shandong Province of China under Grant No. 292. In addition, the authors would like to thank the reviewers for their valuable comments and suggestions.

REFERENCES

[1] Jaideep R, Anupama R. Understanding Web Service. IT Professional, Volume 3C. Washington, DC: IEEE Computer Society,2001.77-78.

[2] An Yang, Guan Jihong,Zhao Bo. An Approach for Web Service Matchmaking Based on DAML-S[J]. Journal of Fudan University(natural science), 2004,43 (5): 938-940.

[3] Blaze M,Feigenbaum J. Decentralized trust management［EB/OL].［2008-10-10]. http://www.cs.utsa. edu/winsboro/teaching/CS6463-S06/Papers/BFL96.pdf.

[4] Zhao Rui-zhen,Song Guo-xiang.An Improved Method for White Noise Reduction Based On Wavelet Transform[J].Journal of Xidian University(natural science),2000,27(5):619-622.

[5] Ma Xiao-ning, Feng Zhi-Yong, Xu Chao. Trust-Based Access Control in Web Service[J].Computer Engineering, 2010,36(3):10-12.

[6] Januszewaki K, Mooney ED.UDDI technical white paper [EB/OL].http:// www. uddi. org/pubs/Iru UDDI Technical White Paper.pdf,2002-09-06.

[7] Mohammad Rostaml, Esmaell Bagheri. Web Services Interoperate as Distributed Systems Based on Trust. 2011 International Conference on Information Communication and Management (ICICM2011), October, 14,2011, Singapore. Vol.16,pp.60-65.

[8] Hu Hao. Research on Distributed Access Control Based on Trust Computer [D].University of Science and Technology of China,2009.

[9] Hu Jian-Li,Zhou Bin,Wu Quan-yuan. Research on Incentive Mechanism Integrateed Trust Management for P2P Networks[J].Journal on Communication, 2011,32 (5): 22-31.

[10] Sun De-Shan,Wu Jin-Pei. Predicting Credibility Based on Support Vector Regression[J].Computer Science, 2003, 30(8):126-127.

[11] Sha Yi, Zhang Lili, Zhu Lichun, Zhang Zhiwei. Routing Protocol Based on Dynamic Exponential Smoothing Prediction in Ad Hoc Network[J].Journal of Chinese Computer Systems,2012,33(3):462-465.

[12] Guo Xiaojing. Research on Security Policy for Web Service[D].Xi'dian University,2009.fessional,Volume 3C. Washington, DC:IEEE Computer Society,2001.77-78.