Study on Trust Model of Internetware System

Tao He[1, a] Yong Wei[1,b] Huazhong Li[1,c] Lina Fang[1,d] Shouxiang Xu[1,e]Defen Zhang[1,f] Junqiang Liu[2,g]

[1] Software College, Shenzhen Institute of Information Technology, Shenzhen, Guangdong 518172,China

[2] Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 210016, China

[a]he_tao@foxmail.com, [b]weiy@sziit.edu.cn, [c]lihz@sziit.edu.cn, [d]fangln@sziit.edu.cn,[e]xusx@sziit.edu.cn,[f]zhangdf@sziit.edu.cn, [g]liujunqiang@nuaa.edu.cn

Keywords: Heterogeneous Software, Trust Model, Time Frame, The Experience Factor

Abstract. We take the overall architecture of internetware on-line evolution model as basic, and study on trust metric model of the software in internetware system. In view of the not accurate results from the rough and existing trust metric model granularity, this paper proposed a multi service and hierarchical dynamic trust metric model based on time frame. Model also offer a method to established time frame weighted factor based on inducing ordered weighted operator, which makes the trust measurement results more accurate. The trust measurement results obtained from the model will be used as decision-making basis for Bias game model.

Introduction

The main software service exists on every point of the Internet, will be collaborated and integrated by a variety of mechanisms into another software forms which can be called internetware[1,2,3]. Internetware offers effective ways to the integration of the heterogeneous resources and make full use of software service from the internet. But with the increasing demand on the function of internetware, the structure, system become more and more complicated, at the same time, environment for running the software changed from the traditional "closed, static, controlled" to "open, dynamic, uncontrolled", the assurance of credibility become increasingly important. But currently there are a lot of shortcomings on like, the constraint mechanism of trust assurance technology in trust relationship, the accuracy of the information, the Rationality of trust attenuation parameters, the systematization of trust evolution model, and the practical of credibility evaluation method and other areas. In view of the above shortcomings, this paper studied on Internetware dependability assurance key technologies which based on the overall architecture of on-line evolution model of Internetware, and study on trust metric model of the software in internetware system network configuration software system between the trust metric models. In view of the existing problems that the rough trust metric model makes the test results is not accurate enough, this paper proposed a multi service hierarchical dynamic time frame based on time model.

An Internetware System Evolution Model

Internetware is an alliance which distributed in an open, dynamic network environment, provided by third party, and has a main body with service characteristics to interconnection. The experts give the basic model [4] of internetware according to the characteristics. The model divides the Internetware into goals layer and control layer, at the same time to ensure the system security through the trusted security mechanism. On the target layer, decides system part which including traditional software, there is also a display description of environmental information. The system part includes the software entity with the services characteristics and the links for these entities. On the control layer, including the perception module for the environment changes and evolution module based on control system. The perception module includes detector and a table which to search the interest, and the evolution module is to control the software entity through effectors. The main difference between internetware and the traditional software is that the change of environment

and requirements from users effect on whole system, the changed requirements can be achieved by changing the operation of the target layer system; and to the environment changes, can be achieved by running the control system to adjust and evaluate, which to further meet the requirements from the users. Therefore, networkware is a cycle process which to achieve the stage goal from users, interact with environment, and evaluate and adjust with system, and then achieve the new stage goal of the users [5]. The concept model of networkware is shown as figure 1:

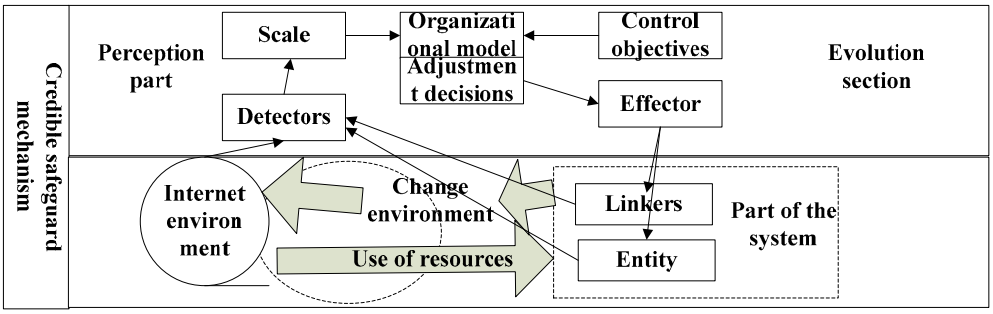

Figure 1: The concept model of networkware

Multi Service and Hierarchical Trust model of Internetware System Based on Time Frame

Multi service and hierarchical trust metric model of internetware system based on time frame: This paper will offer a measurement model of multi service and hierarchical trust model and according to the global service weight table, this model will assign different weights according to different levels of service; and establish the "client" and "server" trust value for each software entities; engage in experience factor into the model to solve the trust degree problems caused by experience difference; at the same time, as the time will also effect on trust, the time will be divided into several time frames, assign weighting factor for each time frame by the induced ordered weighted averaging operator to get the overall trust between nodes. A fine-grained analysis makes the dynamic trust model can accurately reflect the dynamic trust relationship between nodes.

Service set of networkware system can be expressed as $S = \{S_a, S_b, \ldots S_m\}$,among which $S_i = \{S_{i1}, S_{i2}, \ldots S_{in}\}$ means service set provided by software entity i, weights set of system service can be expressed as $K = \{\kappa_a, \kappa_b, \ldots \kappa_d\}$,among which $\kappa_i = \{\varphi_{i1}, \varphi_{i2}, \ldots \varphi_{in}\}$ means the corresponding weight owned by set S i

In the t time frame, software entity a will be a service provider, and the software entity b and Sa interact several times in every service, the number Qa={qai,qa2,…， qan}, among which cooperation times for entity b Ea={ eai,ea2,…， ean }. In the time frame t, direct trust value from entity a to entity b can be expressed as:

$$D^t(a_{se}, b_{cl}) = \sum_{1 \le i \le n} \varphi_{ai} e_{ai} / \sum_{1 \le i \le n} \varphi_{ai} q_{ai} \quad (1)$$

It is the same that in the t time frame, the direct trust degree from the entity a, as a service requestor, to entity b, can be expressed as below:

$$D^t(a_{cl}, b_{se}) = \sum_{1 \le i \le y} \varphi_{bi} e_{bi} / \sum_{1 \le i \le y} \varphi_{bi} q_{bi} \quad (2)$$

Here, Qb={qbi,qb2,…， qbn}shows the interaction times of entity a and entity b in the service of Eb={ eab,eb2,…， ebn }shows cooperation times of entity b in different service.

Within the time frame t, the indirect trust number between entity a and entity b, can be valued by the software entities which had interactive experience on entity b within time frame t. The calculation formula of entity a, as a servicer and requester, and entity b are:

$$V^t(a_{se},b_{cl}) = \sum_{c\in l_{se}(b)} \zeta(a,c_{RE}) D^t((c_{se},b_{cl})) / \sum_{c\in l_{se}(b)} \zeta(a,c_{RE}) \quad (3)$$

$$V^t(a_{cl},b_{se}) = \sum_{c\in l_{se}(b)} \zeta(a,c_{RE}) D^t((c_{cl},b_{se})) / \sum_{c\in l_{se}(b)} \zeta(a,c_{RE}) \quad (4)$$

Here, lse(b) expresses the entity sets who has offer service to b within the time frame t, lcl(b) expresses the entity sets who has request service from entity b. $\zeta(a,c_{RE})$ shows the recommendation trust degree from entity a to entity c, $D^t((c_{se},b_{cl})$ t represents within time frame t, the trust degree offered from entity c, as the service provider, to the entity b, entity $D^t((c_{cl},b_{se})$ the trust degree offered from entity c, as the service requester, to the entity b.

The total trust value from entity a to entity b will be decided by trust value of continuous time frame, here we introduce concept of time frame window, n represents the size of the window, it will reflect the ignorance degree of the entity a, if the entity a only be interested in events happened recently, then decrease n, if the entity a needs to think about earlier events comprehensively, then increase n. calculation formula for total trust value from entity a to entity b within continuous time frame is as follows:

$$T^t(a_{se},b_{cl}) = \sum_{i=t-n} \xi^i * R^i(a_{se},b_{cl}) \quad (5)$$

$$T^t(a_{cl},b_{se}) = \sum_{i=t-n} \xi^i * R^i(a_{cl},b_{se}) \quad (6)$$

Updating the recommendation trust value of introducing experience factor: In this paper, we update the recommendation trust value through the different evaluation of from entity a to entity b within time frame. To omit the space, here we only give the calculation formula of entity a, as a service provider, to entity c, also as service provider. Base on the calculation formula who provides credibility, to improve the original formula, we introduce relative experience factor $\delta^1(a_{se},c_{se})$, which can solve above problem very well. it can reflect experience difference between the node a and node c, the calculation formula is as follows:

$$\delta^1(a_{se},c_{se}) = \frac{\arctan(m_t(a_{se},c_{se})/h_0)}{\arctan(m_t(c_{se},c_{se})/h_0)} \quad (7)$$

h 0 is a threshold value, which is to define individual experience of node c who participated in recommendation, $m_t(a_{se},c_{se})$ represents within the time frame t, the interacting times between node c, as the service node, with node b. it is requested that only in $m_t(a_{se},c_{se}) \geq h_o$ h, node a can accept node c. according to the function range of arc tangent when $\delta^1(a_{se},c_{se}) \in [0,2]$, that can show the experience of node a is more than node C. The introduced experience factor can prevent the incorrect evaluation of entity nodes caused by the lack of experience. The formula of updating the recommendation trust value after introducing the experience factor is as follows:

$$\varsigma(a,c_{re}) = \begin{cases} \varsigma(a,c_{re}) + \dfrac{1-\varsigma(a,c_{re})}{2} \left|1 - \dfrac{diff(a_{se},c_{se})}{\theta}\right| \delta^1(a_{se},c_{se}), diff(a_{se},c_{se}) < \theta \\ \varsigma(a,c_{re}) + \dfrac{1-\varsigma(a,c_{re})}{2} \left|1 - \dfrac{\theta}{diff(a_{se},c_{se})}\right| \delta^1(a_{se},c_{se}), else \end{cases} \quad (8)$$

Experiment Verification and Results Analysis

To verify the performance of the model, in this paper, we used the Netlogo[9] platform to make a simulated network environment, mainly verify from the two aspects, one is dynamic adaptability and accuracy of the model, the other one is the behavior on inhibition of malicious node. Condition: processor - Inter Core2 frequency 2.66GHz; -2G memory; disk -160G; operating system: Win7 system; simulated experiment platform: Netlogo platform (single); summary, drawing tools: Matlab12.0. in this experiment, in the simulated network, 500 nodes will be installed. of the interaction times will be 100 for each node, totally 5000 times among nodes. After a certain number of node interaction, then sample the trust data information, and input the data into Matlab, to analysis the results, until reach the recommended interaction times. There are two entity nodes in this simulation scenario: GB (good behavior nodes) and BB (bad behavior nodes), which is to verify the model ability of the adaptability and accuracy and inhibit the malicious node. The node sets in the whole system can be shown as Nodec Nodec = {e i|1≤ i ≤ N}, then the average trust value of such nodes within time frame t is as follows:

$$trust = (\sum_{i=1}^{N}(\sum_{j \in C_{se}(i)} T^t(j,i) / | C_{se} |) / | Node_c | \quad (9)$$

Within the time frame t, the total interaction times of all the nodes in the system is M, the total number of successful interaction is S, so the successful collaboration rate is: w=s/M.

Figure 2, figure 3 and figure 4 all show the changes status of average trust value of malicious interaction node of the two dynamic change behavior. We can see that the trust values of nodes is only about 0.5. Average trust values of the nodes did not truly reflect the malicious node cooperation strategies. MSCTrust model has very strong ability to adapt dynamic environment, also can reflect quickly according to the nodes change, at the same time, through the granularity model, the no cooperation strategy can be recognized efficiently, which makes the trust evaluation value of the model more accurate.

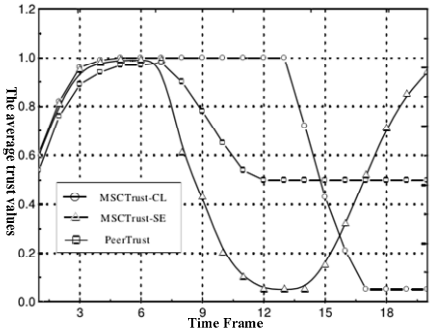

Figure 2 average trust value change with increasing node time

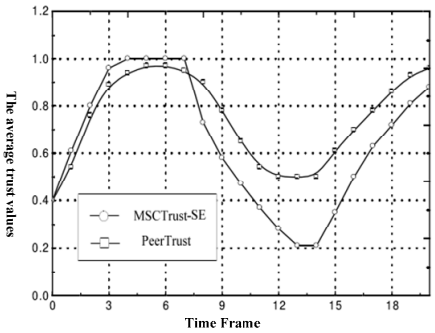

Figure 3 average trust value change with increasing node time Figure

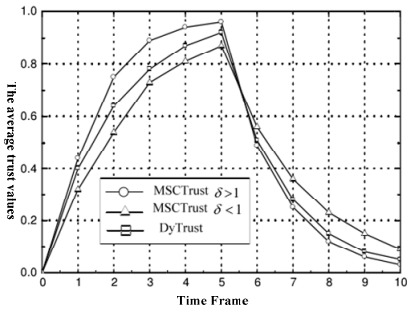

Figure 4 average recommendation trust value change with increasing node time Figure

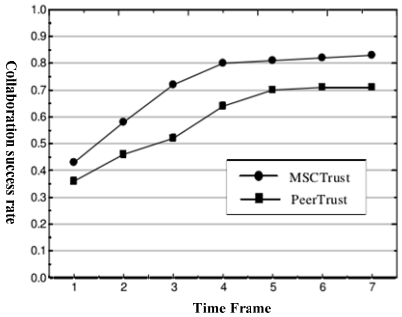

Figure 5 successful cooperation change with increasing node time

From Figure 5, we can see that with the increasing time, the successful cooperation times of the system also increased, and eventually count 0.8. Compared with the PeerTrust model, the

MSCTrust model makes the successful cooperation rate higher. The DMI node has to choose cooperation strategy when the trust value is less than 0.6. Strict Trust Measurement makes nodes in the system select more often which improve the overall performance of the system.

Conclusion

According to the problems caused by rough model granularity and individual experience difference and other problems of existing trust model, we proposed a trust model of multi service and classification dynamic based on the time frame. Firstly, have an overall introduction and summery on rusted and relevant knowledge, then gives the trust management framework for software entities, with this basis, think of that different services have different weights, different software entities have different roles, make a fine-grained analysis on trust metric measurement data based on time frame, and gives the recommendation credibility updating calculation based on experience factor and calculator for time frame weight based on induced ordered weighted operator. Finally, in the simulation experiment, through dynamic adaptability and accuracy of the model and ability to inhibit the malicious node, we verify the validity of the model.

Acknowledgments

This work was supported in part by a grant from Harbin Institute of Technology Robotics and System National Key Laboratory (SKLRS-2012-MS-06), Shenzhen Science and Technology Program (JCYJ20120615101640639, JCYJ20120615102526732 and JC201105190849A), Team of Scientific and Technological Innovation of Shenzhen Institute of Information Technology (CXTD2-002), Natural Science Foundation of Guangdong Province, China (S2011040000672, S2013010013779, S2012040006900, S2013010014543), Guangdong Vocational Education Information Technology Fund(XXJS-2013-1019),Teaching Research Project of Shenzhen Institute of Information Technology(JY2013106), The central university basic scientific research business amount of special funds(NS2014066)，Research Fund of Shenzhen Institute of Information Technology(JY2013106, JY2014B01)， Research and Cultivation Project of Shenzhen Institute of Information Technology(lg201410).

References

[1] Lv Jian. Research and Development of Networkware of [J]. Information Science, 2011, 36 (10): 1037~1080

[2] Yin Guisheng. Multi Strategy and Trusted Model of Internetware Wright-Fisher[J]. Journal of Software, 2012,23 (8): 1978-1991

[3] Dong Yuxin, Study on the Trusted Evolution Model of Internetware [D]. Doctoral Dissertation of Harbin Engineering University,2011.

[4] Li Xiaoyong. Trust Quantification Model in Trusted Network Based on Multiple Decision [J]. Chinese Journal of computers, 2009,32 (3): 405-416.

[5] Shen Peng Study on Protocol Conformance Testing Based on the Finite State Machine model. [D]. Beijing: Beijing University of Posts and Telecommunications, 2013

[6] Gao Jideng. Credible Autonomous Service Coordination Model and Application Development Structure [J]. Information and Science, 2009,39 (11): 1146-1175

[7] Yan Guiling. Modeling Method Based on Monitoring and Trusted Networkware[J]. Computer Engineering and Science, 2013,2 (12): 112-115.

[8] Wang Shuyin. Trust Model Study on Internetware [D]. Harbin: Harbin Engineering University, 2013

[9] Si Guannan. Key Technology Research on the Assurance of Internetware Dependability [D]. Tianjin: Nankai University, 2012