http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (18): 4523-4528, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4523.4528

Normal Cloud Model Based Reputation Quantification in Trusted Networks

Yang Zhi-xiao and Fan Yan-feng
College of Information Science and Engineering, Henan University of Technology,
Henan, Zhengzhou, 450001, China

Abstract: In order to quantify node reputation in trusted networks, while considering fuzziness and randomness of the concept and adapting to network changes, a Normal Cloud Model based (NCM) approach is proposed. Node reputation cloud is constructed through inverse cloud generator from Service Satisfaction Degrees (SSDs) in a big window N. With cloud generator of the cloud, certainty degree of each SSD in reputation computation window H is generated. It is random but with stable tendency. SSD's weight is designed based on its certainty degree and attenuation coefficient. The proposed reputation model is able to describe uncertainties in trusted networks, and adapt to network changes. Experiment results show that the proposed model has stable computation result and high performance of anti-attacking.

Key words: Trusted network, cloud model, reputation, random weight, fuzziness

INTRODUCTION

In open networks such as grid, P2P, universal computing, e-commerce, etc., node reputation is an important network interpersonal relationship. It is a key index for decision of access control, service authority, and transaction. Many researchers addressed in quantification models of node reputation in trusted networks. A Power-Trust system was proposed to collect feedback of local nodes and to aggregate them into global reputation (Zhou and Hwang, 2007). It improves the precision of global reputation and its aggregation speed through so called "look ahead" randomly walking strategy. Some models calculated feedback trust according to hierarchical relationship of trust chains (Li *et al*., 2009). Normal Cloud Model (NCM) based method was proposed to describe fuzziness and randomness of reputation evaluation, to assist customer's shopping decision (Wang *et al*., 2010). Node reputation is decided in essence by the ability that it continuously provides successful services. Its service providing has the performance of clustering. An honest node always provides successful services; a dishonest one, by contrast, its initiative of providing successful services is low. Although it would influence on reputation of a node when it occasionally provides service with quality being opposite to those of common, the changes should not decide its performance inversely.

Node reputation is the aggregation of service satisfaction degrees (SSDs) evaluated by other nodes of a network. SSDs from evaluation nodes, i.e. service acceptors, have the uncertainties of fuzziness and randomness. For example, for interval [0, 1], 1 indicates fully satisfaction; 0, by contrast, fully dissatisfaction. Then how is the service satisfaction extent of SSD = 0.7? If a service acceptor wants to express the same satisfaction extent, does it submit a same SSD value (such as 0.7) every time? In other words, if a service acceptor submits the same SSD value (such as 0.7) for multiple services, does it express the same extent of satisfaction? Further, for an obtained SSD value which obviously deviates from the average of those a service provider obtained, is it an honest evaluation or a dishonest one? For an SSD value which approximates the average, must it be an honest evaluation? Current methods cannot solve the problems.

Fuzzy set theory can describe uncertainty of fuzziness with logic value interval [0, 1]. But its membership function is selected according to people's experience. Once a membership function is decided, its output is exact. It cannot describe randomness.

For the openness of large scale distribution systems, node reputation is easily to be attacked. Some researches proposed to filter SSDs obviously deviating from even value (Tian *et al*., 2008). But the filtering criterion cannot ensure that an abandoned SSD value must be a dishonest evaluation, and a kept one, an honest. Service levels were introduced to reduce cheating on important services (Li and Gui, 2009). But the model has the deficiency of lag. Its anti-attack ability is limited.

NCM Li *et al*. (1995) is able to quantify fuzziness and randomness of a qualitative concept. It adopts three parameters, i.e., expected value Ex, entropy En, and hyper

Corresponding Author: Yang Zhi-xiao, College of Information Science and Engineering, Henan University of Technology, Henan, Zhengzhou, 450001, China

entropy He, to describe the two uncertainties of a qualitative concept. NCM uses certainty degree, which is a random number but with stable tendency, to describe the reliability of a drop representing a concept. The study proposes to construct reputation cloud for a node in a large window. Then aggregate reputation from SSDs in a small window. With cloud generator, SSD weight is designed based on its certainty degree and attenuation coefficient. The reputation model follows uncertainties in service satisfaction evaluation. It has good performance of anti-attacking.

REPUTATION MODEL

In the study, a node's reputation is the aggregation of SSDs submitted by other nodes those directly obtain services from it, whether on the depth dimension or the breadth dimension. The depth dimension means SSDs submitted by one service acceptor, while the breadth one, by all service acceptors. To adapt to node performance changes, the attenuation of SSDs is considered. There is Definition 1. Node reputation R. Let $E = \{e_1, e_2, \ldots, e_N\}$ denote the node set of an open network. $\forall e_j \in E$, $\Omega_j \subset E$ $(\Omega_j \neq \varphi)$ denotes the set of nodes those directly obtain service from e_j. In window H, SSDs of nodes in Ω_j to e_j is denoted with $T_H = \{T_i | T_i \in [0,1], i=1, 2, \ldots, H\}$. In the window, i = 1 means the oldest SSD; i= H, by contrast, the current. The reputation of e_j is:

$$R = \sum_{i=1}^{H} \omega_i T_i \quad (1)$$

In the equation, Ω_i is the weight of SSD T_i. It follows:

$$\omega_i \in [0,1], \sum_{i=1}^{H} \omega_i = 1$$

Reputation model of Eq. 1 is expected to consider fuzziness and randomness of service satisfaction, and to have high anti-attack ability. The key problem is how to design weights for SSDs in computation window H. Following proposes a NCM based weight design.

NCM BASED REPUTATION MODEL

Introduction to NCM: Cloud model is introduced to quantify fuzziness and randomness of a qualitative concept, since the two uncertainties are always together with each other. There is:

Definition 2: Suppose there is a qualitative concept C associated with quantitative universal set U. x U is a random realization of the concept. $\mu(x)$ [0,1] is the certainty degree of x representing concept C. It is a random number but with stable tendency. There is:

$$\mu: U \rightarrow [0,1], \forall x \in U, x \rightarrow \mu(x)$$

The distribution of x on quantification domain U is called a cloud, denoted as C(X). Call x a drop of cloud C(X).

Cloud model defined above has three characteristics. The first, a cloud is the distribution of random variable X on quantitative domain U. However, X is not a simple random variable of probability. In fact, for any realization $\forall x \in U$, it has a certainty degree $\mu(x)$, which is also a random variable other than a exact value. The second, cloud is composed of many drops. Cloud drops have no order. A drop is a realization of qualitative concept C. C is described by cloud C(X) with many drops. Bigger is the number of cloud drops, more obvious are the characteristics of concept C. The third, certainty degree μ of a drop indicates the extent it is able to represent concept C. Of course, higher is its value, bigger is the extent.

Cloud model adopts three parameters to quantitatively describe the overall characteristics of a qualitative concept. They are expected value Ex, entropy En, and hyper entropy He. Ex is the dot which can mostly represent concept C on domain U. En indicates fuzziness and randomness of the concept. It shows drop's value range in domain space possibly accepted by the concept, while indicating drops' disperse extent on the domain. A high En value means a rough concept with high randomness. He is the measurement of uncertainty of entropy En. It indicates the randomness of certainty degree under given drop value in domain U. With the three numerical characters, a cloud model is denoted with vector C(Ex, En, He).

If drop x and the three parameters follows:

$$x = \text{Norm}(Ex, En^2) \quad (2)$$

$$En' = \text{Norm}(En, He^2) \quad (3)$$

$$\mu = e^{-\frac{(x-Ex)^2}{2En'^2}} \quad (4)$$

it is called a Normal Cloud Model (NCM). In the equations, Norm() means a normal distribution.

A NCM follows so called "3 En rule", because drops locating within [Ex-3En, Ex+3En] take up to 99.99% of the whole quantity and 99.74% of the total contribution to the concept. So drops locate out of the interval are neglected. Normal cloud generator (CG) is to generate drops (x_i, μ_i) with given cloud C (Ex, En, He). Inverse cloud generator

(CG^{-1}) is to estimate parameters C (Ex, En, He) through many drops, i.e., the data pairs (x_i, μ_i).

SSD weight based on NCM: In a trusted network $E = \{e_1, e_2, \ldots, e_N\}$, $\forall e_j \in E$, denote its all SSDs in window N (N>>H) with $X = \{x_i | x_i \in [0,1], i = 1, 2, \ldots, N\}$. Its quantitative universal set is U = [0, 1]. There is a qualitative concept, i.e., the reputation of e_j associated with domain U. The mean of sample set X is:

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

The first order sample absolute central moment is:

$$M_1 = \frac{1}{N}\sum_{i=1}^{N} |x_i - Ex| \tag{6}$$

The sample variance is:

$$S^2 = \frac{1}{N-1}\sum_{i=1}^{N} (x_i - Ex)^2 \tag{7}$$

With above equations, a cloud's parameters can be estimated. The estimation of expected value Ex is:

$$\hat{Ex} = \bar{X} \tag{8}$$

The estimation of entropy En is:

$$\hat{En} = \sqrt{\frac{\pi}{2}} M_1 \tag{9}$$

The estimation of hyper entropy He is:

$$\hat{He} = \sqrt{S^2 - En^2} \tag{10}$$

With above equations, parameters of reputation cloud can be estimated as $C(\hat{Ex}, \hat{En}, \hat{He})$. $\hat{Ex}$ is the drop, i.e., a SSD in domain U that can mostly represent the reputation of e_j in window N. $\hat{En}$ is the measurement of the concept's fuzziness. A big entropy value means a rough reputation. On the other hand, it is also the measurement of randomness of the concept. It indicates the disperse extent of drops within domain U. $\hat{He}$ indicates the stability of $\hat{En}$. It describes the randomness of certainty degree of a drop under given value.

NCM based SSD weight design: In the big window N, parameters of e_j's reputation cloud can be estimated from collected SSDs. In the computation window H, with CG of cloud $C(\hat{Ex}, \hat{En}, \hat{He})$, certainty degree of SSD T_i (i = 1, 2, …, H) can be produced by:

$$En' = Norm(\hat{En}, \hat{He}^2) \tag{11}$$

$$\mu(T_i) = e^{\frac{(T_i - \hat{Ex})^2}{2En'^2}} \tag{12}$$

The attenuation coefficient of SSD T_i is linearly designed as:

$$\begin{cases} r_i = 1, i = H \\ r_{i-1} = r_i - a, i \neq H \end{cases} \tag{13}$$

In the equation, a [0,1]. $\forall r_i > 0$. A big certainty degree indicates a high reliability that the drop represents e_j's reputation. So a SSD with big certainty degree should be set with high weight. Based on the principle and attenuation coefficient in Eq. 13, the weight of T_i is designed as:

$$\omega_i = \frac{r_i \mu(T_i)}{\sum_{i=1}^{H} r_i \mu(T_i)} \tag{14}$$

For the randomness of certainty degree $\mu(T_i)$, weight ω_i obtained by Eq. 14 is also random. But the randomness has stable tendency. With Eq. (1), e_j's reputation can be calculated. Sliding windows N and H, parameters of e_j's reputation cloud will be re-estimated. Weights in reputation computation window H will also be refreshed. Because ω_i is decided in essence by collected SSDs, human subjectivity is avoided in weight design of reputation model. Further, the model is able to adapt to network changes.

NCM based node reputation algorithm: With above works, the NCM based node reputation algorithm in trusted networks is described as:

- **Step 1:** Input a, N, H
- **Step 2:** Input X. Calculate $\bar{X}$, M_1, S^2, $C(\hat{Ex}, \hat{En}, \hat{He})$
- **Step 3:** Input T_H. Calculate En', $\mu(T_i)$, r_i, Ω_i
- **Step 4:** Calculate R
- **Step 5:** Slide windows N and H. Go to step 2

EXPERIMENT RESULTS AND ANALYSIS

Analysis to reputation cloud describing concept reputation: Figure 1 presents three estimated reputation clouds, which are C(0.7, 0.02, 0.05), C(0.7, 0.1, 0.05) and C(0.7, 0.02, 0.02), respectively. They have the same

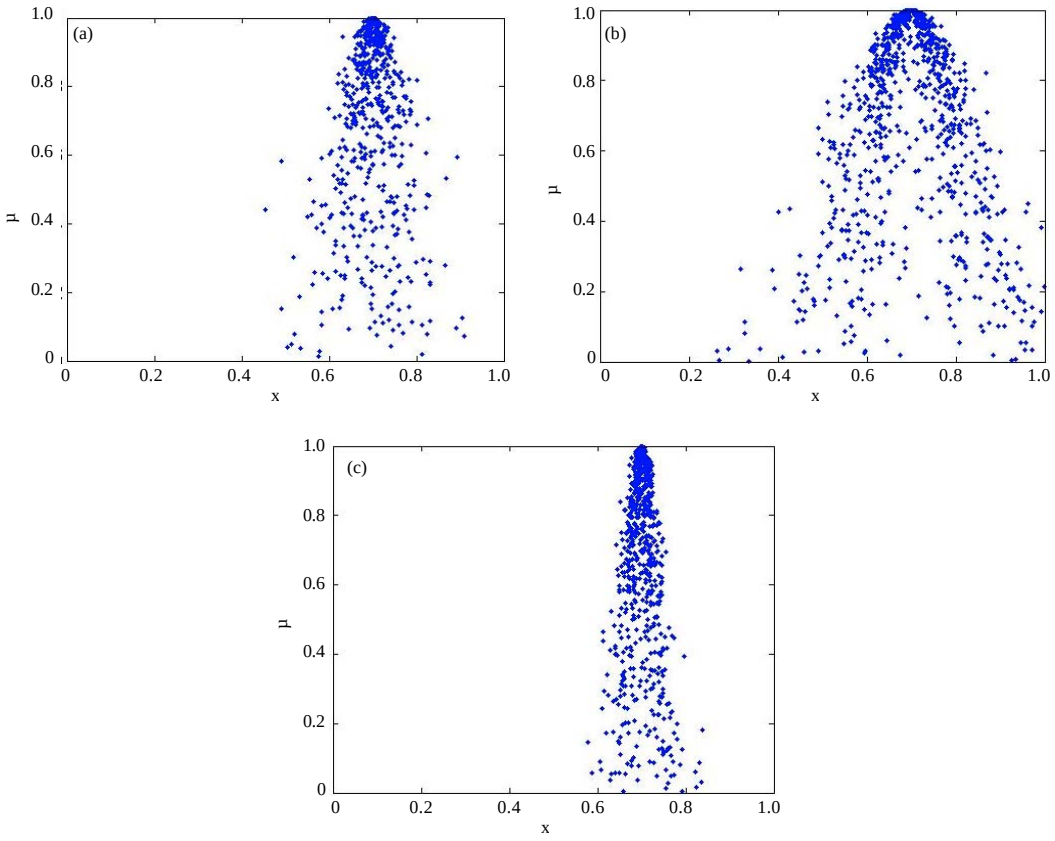

Fig. 1(a-c): Reputation clouds (a) C(0.7, 0.02, 0.05), (b) C(0.7, 0.1, 0.05) and (c) C(0.7, 0.02, 0.02)

expected value 0.7. So 0.7 is the drop in domain U that can mostly represent the three concepts. Clouds C(0.7, 0.02, 0.05) and C(0.7, 0.1, 0.05) have the same hyper entropy value 0.05. But the former cloud has smaller entropy value (0.02) than the later does (0.1). So the drops in the later cloud are more disperse. The reputation it represents is rough. Clouds C(0.7, 0.02, 0.05) and C(0.7, 0.02, 0.02) have the same entropy value0.02. But the hyper entropy value of the former cloud (0.05) is bigger than that of the later (0.02). Although the two concepts have the same fuzziness, drops in the former cloud are more disperse along the certainty degree axis than those in the later.

Set window N = 1000. With a simulated SSD sample set X, the reputation cloud is estimated as C(0.6921, 0.0435, 0.0433). Figure 2 presents respective 100 realized certainty degrees at drops 0.69, 0.6, and 0.4 under the cloud. Drop 0.69 is close to expected value 0.6921. In the 100 realized certainty degrees, most are close to 1. But each value is different from the others. Even a few values are very low. For drop 0.4, its 100 realized certainty degrees appear the similar feature but close to 0. Certainty degrees of drop 0.6 are the most disperse in the three drops. The figure shows that certainty degree is random

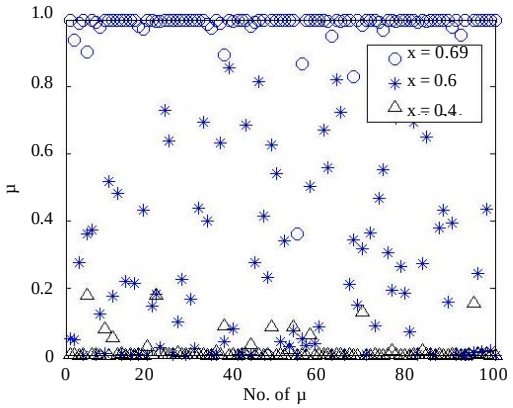

Fig. 2: Distribution of certainty degree μ of drops in cloud C(0.6921, 0.0435, 0.0433). 100 realization at each x = 0.69, 0.6, 0.4

but with stable tendency. It indicates the uncertainty of reliability that a drop, i.e., a SSD, is able to represent a node's reputation.

For the randomness of certainty degree, weight ω_i in Eq. 14 is also a random number for given SSD value T_i.

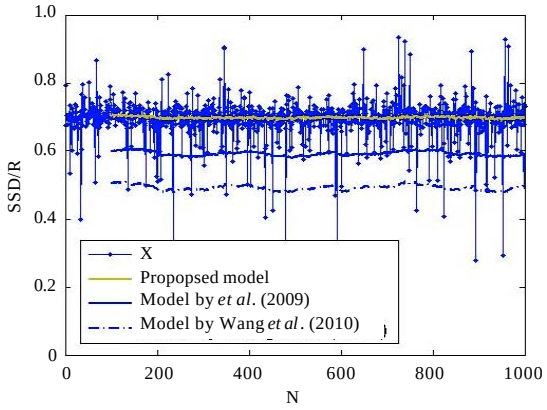

Fig. 3: Reputation computation results. To easily observe, results of Li *et al*. (2009) and Wang *et al*. (2010) are moved downside by 0.1 and 0.2 units, respectively

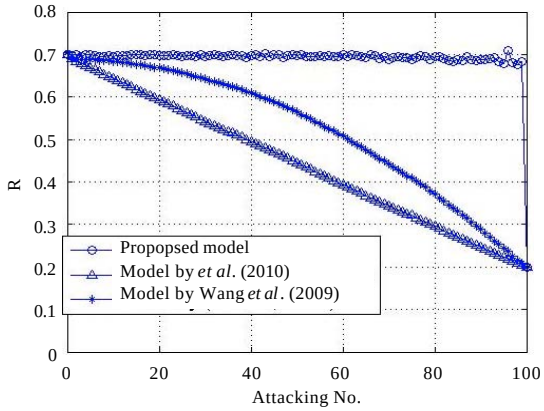

Fig. 4: Anti-attack results. Attack value is 0.2

The characteristic introduces the uncertainties in service satisfaction evaluation into the reputation model. So the computation results are flexible other than being exact. But the flexibility is not too big for the stable tendency of certainty degree's randomness. Because reputation cloud is estimated from SSD samples, the model follows the uncertainties and adapt to changes of networks.

Analysis to reputation computation results: Set reputation computation window H = 100. With SSD sample set X, the reputation computation results by proposed method, by model of Li *et al*. (2009), and by model of Wang *et al*. (2010) are present in Fig. 3. The three models set attenuation coefficient with a = 1/H in Eq. 13. The figure shows that although SSD undulates greatly at some times, the computation results are stable with proposed method. Results of Li and Gui (2009) and Wang *et al*. (2010), by contrast, undulate obviously.

Anti-attack results: Collect 100 SSD samples in X with reputation computation window H. Let 0.2 be an attacking value. Replace SSDs with 0.2 step by step from the first SSD in the window. The computation results are present in Fig.4. In the figure, the vertical axis is calculated reputation. The horizontal axis is the number of attacking value, i.e., 0.2.

The figure shows that the results of proposed method are very stable, even the attack number is very big. However, reputation by Li *et al*. (2009) and Wang *et al*. (2010) decrease rapidly according to the increasing of attack number. Although the model of Wang *et al*. (2010) also adopted NCM, it is easy to be attacked because it uses the same small window H for estimating cloud parameters. The proposed method appear good performance of anti-attacking.

CONCLUSION

A NCM based method is proposed to calculate node reputation in trusted networks. A node's reputation cloud is constructed from SSDs in a big window N. With CG of the cloud, certainty degrees of SSDs in reputation computation window H can be generated. Certainty degree is random but with stable tendency. A SSD with a high certainty degree shares big weight. In window H, SSD's weight is designed based on certainty degree and attenuation coefficient. It is also random but with stable tendency. Because the parameters of reputation cloud are estimated from SSD samples, the NCM based reputation model is able to deal with fuzziness and randomness of the concept, while adapting to network changes. Experiment results show the proposed model have stable computation result and high performance of anti-attacking.

ACKNOLEDGEMENT

This study is supported by the National High Technology Research and Development Program of China under Grant No. 2012AA101608, the Science-Technology Project of Zhengzhou of China under Grant No. 2010GYXM364, and the High Level Talent Foundation of Henan University of Technology under Grant No. 2010BS027.

REFERENCE

Li, D.Y., H.J. Meng and X.M. Shi, 1995. Membership clouds and membership cloud generators. J. Comput. Res. Dev., 32: 15-20.

Li, M.C., B.Yang, W. Zhong, L.L. Tian, H. Jiang and H.G. Hu, 2009. Grid dynamic authorization model based on feedback mechanism. Chinese J. Comput., 32: 2187-2199.

Li, X.Y. and X.L. Gui, 2009. Trust quantitative model with multiple decision factors in trusted network. Chinese J. Comput., 32: 405-416.

Tian, C.Q., S.H. Zou, W.D. Wang and S.D. Cheng, 2008. A new trust model based on recommendation evidence for P2P networks. Chinese J. Comput., 31: 270-281.

Wang, S.X., L. Zhang and H.S. Li, 2010. An evaluation approach of subjective trust based on cloud model. J. Software, 21: 1341-1352.

Zhou, R.F. and K. Hwang, 2007. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans. Parallel Distrib. Syst., 18: 450-473.