Trust Computation Based on Fuzzy Clustering Theory

Shunan Ma[1], Jingsha He[2] and Yuqiang Zhang[1]

[1]*College of Computer Science and Technology*
[2]*School of Software Engineering*
Beijing University of Technology, Beijing 100124, China
msn1679@126.com, jhe@bjut.edu.cn

Abstract

Trust is part of our daily life and thus can be used as a mechanism for providing security in computer networks. In this paper, by considering the dynamic nature of trust, especially the temporal and spatial characteristics in security of society, we describe trust from four factors: access time, place, history behavior and risk control strategy and then apply fuzzy clustering method and information entropy theory to design a weight allocation algorithm for these factors to compute a value for trust.

Keywords: *trust, security, fuzzy clustering*

1. Introduction

Trust is an important aspect of decision making for Internet applications and, in particular, influences the specification of security policy [1]. Trust models have been proposed to control anonymity, unpredictability and uncertainty [2, 3]. The concept of trust is originally derived from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [4]. Blaze first introduced the notion of "trust management" and identified trust as a separate component of security services in networks [5]. In recent years, many researchers have also applied trust to solving network security problems in which measurement of trust relationship between entities in networks has become a key issue. However, the application of classic mathematics functions to compute trust values often leads to inaccuracy. The reason is that trust has the nature of subjectivity and fuzziness.

In this paper, by simulating the temporal and spatial characteristics of security in the human society, we describe the trust includes four factors: access time, place, history behavior and risk control strategy. We will apply fuzzy clustering and entropy theory to design a weight allocation algorithm for these factors and show through simulation that our proposed method of trust computation is feasible.

2. Trust computation

The purpose of applying trust to control access to information and services is to prevent "illegal" subjects from accessing resources as accurately as possible. From another perspective, the access behavior of an "illegal" subject is similar to crime in law since they both violate the constraint defined for the actions. Prior research has shown that crime has significant time and space features [6, 7]. For example, November and December are the period in which most criminal cases occur during a year and most criminal cases happen from 6pm to 12pm in a day. Furthermore, the crime rate is higher in urban areas. In sociology, trust on a person who has criminal record is significantly lower than that on an ordinary individual. In our study, we use the IP address of a subject to denote the place factor.

Trust exhibits three characteristics: dynamism, subjectivity and ambiguity. Risk control refers to the ability of control and repair of an object after unauthorized access takes place. The impact of risk control factor on trust evaluation is closely related to the security system of an object. Generally speaking, the higher the object's security level, the stronger the risk control ability and the higher the subject's trust value.

Given each factor of trust, suppose every factor's trust value is $T_0, T_1, ..., T_{n-1}$, respectively, and the weight of each factor is W_i, trust value can be computed as: $T = \sum_{i=0}^{n-1}(W_i \times T_i)$. For different application, factors of trust can be set specifically. In addition, trust computation consists of two parts: determine each factor's trust evaluation method to get each factor's trust value and each factor's weight allocation.

2.1. Evaluation of Trust Factors

According to an object's property and a subject's behavior history information, we can establish tables for the time and place of the trust evaluation rules. For example, the trust value of a subject who accesses a recreation resource during work hours is lower than that during spare time. For accessing educational resources, trust value of a subject whose IP address belongs to an educational network is higher than that to a non-educational network.

According to the property of each resource, time can be divided into n periods. For each time period [ti,tj], we formulate corresponding trust interval [Ti,Tj], which means that when a subject accesses the resource at time t, if ti≤t≤tj, then randomly generate a trust value T∈[Ti,Tj]. To avoid denial of access to an object in high crime periods, we use the following method. For each time period [ti,tj], when the number of accesses reaches a certain value, count the total access number m and fraud number k and the fraud probability in this period is p=k/m. Then, randomly generate a trust value Tx at time x where Tx∈[Ti,Tj]. The trust value of time factor is then

$$T = Tx \times (1 - p). \tag{1}$$

According to the time attribute of resources, trust evaluation table for the time factor is shown in Table 1.

Table 1. Trust Evaluation Table for the Time Factor

Time period	$[t_0,t_1)$	$[t_1,t_2)$	$[t_2,t_3)$	…	$[t_{n-1},t_n)$
Trust interval	$[T_0,T_1)$	$[T_1,T_2)$	$[T_2,T_3)$	…	$[T_{n-1},T_n)$
Fraud probability	p_0	p_1	p_2	…	p_{n-1}

We use IP addresses as the place factor. Subjects can be classified according to the property of an object. For example, subjects can be classified into subjects in the same subnet, domain, important service segment and general service segment. We then formulate the trust evaluation intervals. For each network segment, when the length of access time reaches a certain number, we count the fraud probability in this network segment. For a given IP address, we can use Formula (1) to compute the trust value of the IP factor. Trust evaluation table for the IP factor is shown in Table 2.

Table 2. Trust Evaluation Table for the IP Factor

IP address	Same subnet	Same segment	Important service	…	General service
Trust interval	$[T_0,T_1)$	$[T_1,T_2)$	$[T_2,T_3)$	…	$[T_{n-1},T_n)$
Fraud probability	p_0	p_1	p_2	…	p_{n-1}

The purpose of introducing behavior history is to control the subject who commits fraud after getting access permissions. An object records the subjects who accessed it. Objects can then use these behavior history records as the foundation for a subject's future trust computation. If a subject can access the object, then the object uses access feedback policy. Let S denote access feedback satisfaction degree. An object establishes an access record table to record subjects' access information. The access record table includes: access number, ID, trust values and access feedback satisfaction degree. The access record table is regarded as a subject's "file". Such an access record table is shown in Table 3.

Table 3. Access Record Table

Sequence number	ID	trust				Behavior feedback
		Time	IP	Behavior history	Risk control	
1	Subject i	T_{10}	T_{11}	T_{12}	T_{13}	S_1
2	Subject k	T_{20}	T_{21}	T_{22}	T_{23}	S_2
…	…	…	…	…	…	…
n-1	Subject k	$T_{n-1\,0}$	$T_{n-1\,1}$	$T_{n-1\,2}$	$T_{n-1\,3}$	S_{n-1}
n	Subject j	$T_{n\,0}$	$T_{n\,1}$	$T_{n\,2}$	$T_{n\,3}$	S_n

In the table, Tij is the product of jth factor's trust value and its weight of subject i. The trust value of behavior history is the product of most recently accessed feedback value and its weight. To reduce the access control risk, when a subject first accesses an object, the trust value for the behavior history is defined as 0.5, a middle value.

Objects may use different security policies and the degree of protection may differ, namely, objects have different risk control abilities. An object can formulate the trust value of risk control factor based on its own policy. The basic principle is that the higher the level of security policy, the greater the trust value. Risk control table is shown in Table 4.

Let Tij denote the risk control degree when object i uses security policy j for protection. If the subject's access feedback value is $S \in [0,1]$ in the access record table and the subject accesses object i, then the trust value of risk control factor is

$$T = Tij \times S. \tag{2}$$

Table 4. Trust Evaluation Table for Risk Control

Object	Policy 1	Policy 2	…	Policy n
Object 1	T_{11}	T_{12}	…	T_{1n}
Object 2	T_{21}	T_{22}	…	T_{2n}
…	…	…	…	…
Object *m*	T_{m1}	T_{m2}	…	T_{mn}

2.2. The Weight Allocation Algorithm

Suppose that trust consists of m factors denoted as x={T0,T1,…Tm-1}. We can then design a weight allocation algorithm based on fuzzy clustering method [8] for the factors. The algorithm is described as follows:

(1) Randomly select n history trust records with each of which being initialized and denoted as vi={xi}, i=0,1,…,n-1. These n history trust values can then form a $m \times n$ matrix $X = \begin{bmatrix} T_{00} & T_{01} & \cdots & T_{0(n-1)} \\ T_{10} & T_{11} & \cdots & T_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ T_{(m-1)0} & T_{(m-1)1} & \cdots & T_{(m-1)(n-1)} \end{bmatrix}$ in which each column denotes each factor value. For example, Tij represents the trust value of the ith factor in trust j.

(2) For each row of X, $T_{ij} = \dfrac{T_{ij}}{MAX\{T_{i0}, T_{i1}, ..., T_{i(n-1)}\}}$, where $T_{ij} \in [0,1]$.

(3) Establish an $n \times n$ fuzzy similarity matrix R. For any given rij in R, $r_{ij} = \dfrac{\sum_{k=0}^{m-1}(T_{ki} \wedge T_{kj})}{\sum_{k=0}^{m-1}(T_{ki} \vee T_{kj})}$.

(4) For matrix R, use the Equivalence Closure method [9] to get the fuzzy equivalence matrix H.

(5) Let set $C = \phi$ and hij denote the element of the ith row and the jth column in H. For any given hij, if $h_{ij} \notin C$ and $h_{ij} \neq 1.0$, $C = C \cup \{h_{ij}\}$; $q = \dfrac{1}{|C|}\sum_{k=0}^{|C|-1} C_k$, $l = \max\{C\}$ and $g = \dfrac{(\lfloor l \times 10 \rfloor - \lceil q \times 10 - 0.5 \rceil)}{0.5}$. If $g \le 0$, then $G = q$. Otherwise, $G_i = \lceil q \times 10 - 0.5 \rceil \times 0.1 + 0.05 \times (i-1)$, $i = 0,1,\cdots g-1$; $G = \dfrac{1}{g}\sum_{i=0}^{g-1} G_i$.

(6) Construct a classification matrix B from the fuzzy equivalence matrix H. For any given element bij in matrix B, $b_{ij} = \begin{cases} 1 & h_{ij} \ge G \\ 0 & h_{ij} < G \end{cases}$, search each row of B for any bij=1, j<i. If it doesn't satisfy j<k<i and bik=1, then the ith history trust is integrated into the jth history trust category, namely, $v_j = v_j \cup v_i, v_i = \phi$.

(7) Compute the entropy of n history trust sets, i.e., I= $-\sum_{i=0}^{n-1}\frac{|v_i|}{n}\log_2^{|v_i|/n}$.

(8) Delete each row of the trust matrix X in turn, namely, delete each element of trust to get a new trust matrix Y0,Y1,...,Ym-1. For matrix Yk , k=0,1,...,m-1, perform step (2) to step (7) repeatedly to get values of Gk and Ik. If G=Gk, then Mk= Ik/ Gk. Otherwise, $M_k = \left|\frac{I-I_k}{G-G_k}\right|$, where Mk denotes the dependence of n trust on the kth factor.

(9) According to each factor's impact on history trust, determine its weight $W_i = \frac{M_i}{\sum_{j=0}^{m-1} M_j}$.

(10) Output each factor's weight and terminate the algorithm.

3. Conclusions

According to the dynamic nature of trust, we define trust includes four factors: access time, place, behavior history and risk control strategy. We then applied the fuzzy clustering method and information entropy theory and designed a weight allocation algorithm for the evaluation of the factors of trust to compute the values of trust. In the future, we are going to further enhance and refine our method by adding more factors to make it more widely applicable and through more vigorous analysis and experiment.

References

[1] T. Fan and H. Guo, "Attributed Based Access Control of Collaborative Design Systems. Advanced Materials Research, Vol. 267, pp. 80-85 **(2011)**.

[2] A. Nagarajan, "Dynamic Trust Enhanced Security Model for Trusted Platform based Services", Future Generation Computer Systems, Vol. 27, No. 5, pp. 564-573 **(2011)**.

[3] L. Alboaie and M. F. Vaida, "Trust and Reputation Model for Various Online Communities", Studies in Informatics and Control, Vol. 20, No. 2, pp. 143-156 **(2011)**.

[4] K. S. Cook (editor), "Trust in Society", Russell Sage Foundation Series on Trust, Vol. 2 **(2003)**.

[5] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management", In: IEEE Symposium on Security and Privacy, pp. 164-173 **(1996)**.

[6] F. Wang, "Study on the Comprehensive Treatment of Spatial Blind Areas in Urban Crime", Geographical Research, Vol. 29, No. 1, pp. 57-67 **(2010)**.

[7] G. J. DeLone, "Public housing and the Fear of Crime", Journal of Criminal Justice, Vol. 36, No. 2, pp. 115-125 **(2008)**.

[8] H. Li, "The Foundation of Fuzzy Mathematics and Practical Algorithm", Beijing: Science Publishing House **(2005)**.

[9] J. F. Zhang and B. R. Deng, "Application Fuzzy Mathematics", Beijing: Geological Publishing House, Beijing **(1991)**.

Authors

Shunan Ma is a Ph.D candidate in the College of Computer Science and Technology at Beijing University of Technology, Beijing, China. She received her B.S. degree in Qufu Normal University in 2004 and M.S. degree in Jiangnan University in 2007, respectively. Her research interests include network security and distributed network technology.

Jingsha He is currently a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. He received his doctorate from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking and computer security. His interests include methods and techniques that can improve the security and performance of the Internet as well as wireless networks.