15. Jie He, Yishuang Geng, Yadong Wan, Shen Li, Kaveh Pahlavan, A cyber physical test-bed for virtualization of RF access environment for body sensor network, IEEE Sensor Journal, 2013,10, pp.3826-3836.
16. Wenhua Huang, Yishuang Geng, Identification Method of Attack Path Based on Immune Intrusion Detection, Journal of Networks, 2014,9,pp. 964-971.
17. Guanqun Bao, Liang Mi, Yishuang Geng, Mingda Zhou, Kaveh Pahlavan, A video-based speed estimation technique for localizing the wireless capsule endoscope inside gastrointestinal tract, 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), New York,2014,pp.789-794.
18. Degui Zeng, Yishuang Geng, Content distribution mechanism in mobile P2P network, Journal of Networks, 2014,9, pp,1229-1236.
19. Mingda Zhou, Guanqun Bao, Yishuang Geng, Bader Alkandari, Xiaoxi Li, Polyp detection and radius measurement in small intestine using video capsule endoscopy, 2014 7th International Conference on Biomedical Engineering and Informatics (BMEI), London,.2014,pp.456-458.
20. Gan Yan, Yuxiang Lv, Qiyin Wang, Yishuang Geng, Routing algorithm based on delay rate in wireless cognitive radio network, Journal of Networks, 2014,9, pp.948-955.
21. Guanqun Bao, Liang Mi, Yishuang Geng, Kaveh Pahlavan, A computer vision based speed estimation technique for localiz ing the wireless capsule endoscope inside small intestine, 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Sydney,2014,pp.457-459.
22. Xinchao Song, Yishuang Geng, Distributed community detection optimization algorithm for complex networks, Journal of Networks, 2014,10, pp.2758-2765.

Research on Enterprise Comprehensive Evaluation Model of Subjective Trust Based on Fuzzy Theory

LIU Ta[1], HANG Dong-Ping[1], ZHOU Hang[2]

1.Department of Management, Harbin Institute of Technology , Harbin,150000, China
2.Department of Accounting, Harbin University of Commerce, Harbin,150000, China

Abstract
In view of the features of information trust such as its subjectiveness and uncertainty in the enterprise comprehensive evaluation environment, the author presents a subjective trust evaluation model based on fuzzy theory. The model uses fuzzy theory to get the calculation formula of comprehensive trust evaluation between nodes, introduces time factor and constraint mechanism for bad faith node in trust calculation, calculates comprehensive trust value by using similarity degree reverse weight, and achieves cluster analysis of trust value using fuzzy equivalence relations. The simulation results analysis proves the effectiveness and feasibility of the model mention above, and the simulation comparison verifies that the model can objectively reflect the situation close to the real.

Keywords: SUBJECTIVE TRUST, FUZZY THEORY, ENTERPRISE COMPREHENSIVE EVALUATION, SIMILARITY DEGREE, FUZZY EQUIVALENCE RELATION, COMPREHENSIVE TRUST

Introduction

In recent years, with the rapid development of the Internet, reliable and secure network has become a topic of concern to most users. The openness and complexity of the Internet makes the relationship between subjects very difficult to get reliable guarantee and causes directly the rampant of various fraud on the Internet. Actually, in the real life, interpersonal relationship is built up through mutual trust. However, human being is a creature with strong thinking, so the trust is influenced by its subjective feelings with great uncertainty, i.e. Vagueness. The openness and complexity of Internet brings about many security problems; therefore, a trust evaluation mechanism needs to be introduced to measure the node trust in order to establish a reliable trust relationship and eliminate network security risks. In these years, many specialists presented their trust evaluation models under different backgrounds. Early in 1996, Blaze and some other people presented "fuzzy theory", defined the concept of "trust management", and described trust measurement and problems of trust calculation and comprehensive calculation caused by the requirement that it be recommended by a third party.Trust evaluation model to describe and measure trust relationship based on experience and probability and statistics presented by T. Beth made trust uncertainty equal to randomness. However, this model defines direct trust too strictly neglecting the vagueness of trust itself. Jøsang and some other people introduced the concepts of fact space and notion space to describe and measure trust relationship based on subjective logic trust. Though they gave some guidelines, they all established the model using probability model, which made trust subjectiveness equal to randomness and couldn't reflect the real trust relationship.

1. Summary of Subjective Trust Model

The key of the whole interactive communication lies in the mutual trust in enterprise comprehensive evaluation. Communications between enterprises are based on mutual trust. Trust is the subjective expectations of the body specifically for a particular individual's certain behavior. Trust degree of a particular individual comes from direct interaction experience and recommendation experience by other individuals. In today's open internet environment, like interpersonal relationship, trust relationship between nodes has the features as follows: data will be saved every time nodes in the network communicates with other nodes; trust between nodes is generally relative to its environment; each node in the network can choose communication objects randomly; trust is a conclusion of past communication results and the results and their influences may change as time passes by; in certain time and circumstances, nodes should push reliable recommend lessons for other nodes; when one node pushes malicious recommendation lessons, it should be restricted necessarily.

The subjective trust evaluation model presented in this paper is based on fuzzy theory (Figure 1). Trust relationship between nodes is established based on trust communication process under Agent collaboration. Part 1 is communication between nodes, resulting in direct trust and recommended trust. The database established will be dealt by modeling in Part 2; Part 2 generates the value of comprehensive trust

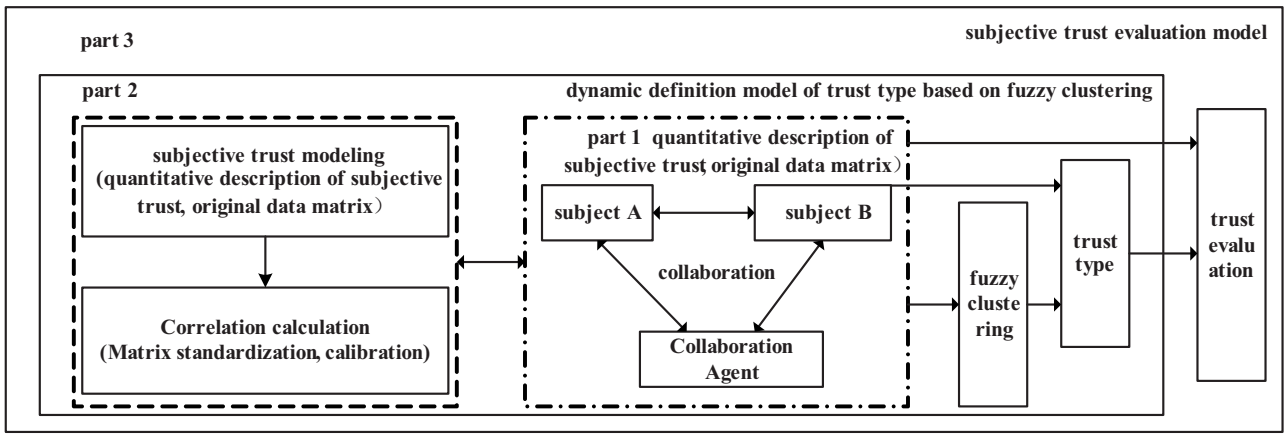

Figure 1. Subjective Trust Model

evaluation by calculation during modeling; Part 3 generates the final trust assessment through comprehensive evaluation value of trust.

2. Subjective Trust Evaluation Method

Trust between nodes can be divided into two kinds: direct trust and recommendation trust. Nodes $X_i(i=1,...,n)$ in the field have been given quantitative description trust through fuzzy theory in the literature, that is to say, trust vector $v(x_i)=(v_{i1},v_{im},...,v_{im},)=(\mu_{i1},\mu_{i2},...,\mu_{im})$, and dynamic definition of trust type has been made. The following is to analyze the trust evaluation between nodes based on trust vector.

2.1. Evaluation of Direct Trust

Generally speaking, direct trust comes from direct communication records between nodes. With these history records, subjective judgment whether the other node is credible can be made. If node *X[i]* communicates with node *X[j]*, *X[i]* can make evaluation about *X[j]*according to its own judgment. Continuous communication like this can generate a direct trust vector $S^t_{ij}=(s^1_{ij},s^2_{ij},...,s^n_{ij})$ which is a repeated contact record. In this vector, *1* represents the latest time of communication record. However, with the change of time, the more ancient the history records are, the less contribution they make to evaluation, so the influence of the size of *n* is great. If the size of *n* is too small, some important records for evaluation is lost; otherwise, too big, the influence of history records is overstated, which may cause inaccuracy of the final evaluation. Combined with trust transfer mechanism, the paper first presents calculation formula for direct trust evaluation.

$$DT_{AB}=\frac{1}{n}\sum_{i=1}^{n}\lambda_i * s^i_{AB} * \phi_{AB} \qquad (1)$$

In this formula, DT_{AB} represents direct trust degree of *A* towards *B*; *n* represents the total number of contact records; λ_i is time factor, representing time factor from the first record to the nth one in direct trust vector $S^t_{ij}=(s^1_{ij},s^2_{ij},...,s^n_{ij})$. $\lambda_i=1-i\sigma$, (*i*=1, 2, …, n), $\lambda_i\in(0,1)$, σ is forgetting factor, $\sigma\in(0,1)$; s^i_{AB} represents the ith direct contact record of node A towards node B; ϕ_{AB} represents constraint factor.

Then, calculation process of direct trust evaluation is as follows:

(1) If no direct communication record between nodes is available, recommendation trust evaluation or the initial setting value is decisive;

(2) Direct trust degree is calculated according to time factor through direct communication records;

(3) When each round of trust degree is updated, evaluation results will be stored in the database in which the direct communication records are checked. If the total number of records exceeds the total number of valid records, the oldest ones should be deleted.

2.2. Evaluation of Recommendation Trust

Direct trust degree is not influenced by recommendation trust from malicious nodes, because all the communication records are produced by node A itself. However, this kind of direct trust can hardly reach credibility close to fact without several rounds of updates. Therefore, aided with recommendation trust between nodes, data can be collected more quickly and the comprehensive evaluation of node A towards node B can be obtained more effectively.

Recommendation trust is a credibility evaluation of node A towards node B through evaluations provided by other nodes. This model adopts the method mentioned in the literature, calculates recommendation trust value based on the direct trust value between the node itself and neighbor nodes by collecting recommendation trust stored in neighbor nodes. Evaluation formula for recommendation trust is:

$$RT_{AB}=\frac{1}{m}\sum_{i=1}^{m}W_i * IT_{iB} * \phi_{iB} \qquad (2)$$

In this formula, RT_{AB} represents commendation trust degree of node A towards node B; m represents the number of neighbor nodes of node A; W_i represents trust weight coefficient of node A towards node B, $W_i=\frac{DT_{Ai}}{\sum_{l=1}^{m}DT_{Al}}$; IT_{iB} represents comprehensive trust degree of node i towards node B; ϕ_{iB} represents constraint factor.

2.3. Evaluation of Comprehensive Trust

Definition: similarity degree is the measure of closeness of two fuzzy sets. Let $\delta(A,B)$ be the closeness of two fuzzy sets A and B, $0\le\delta(A,B)\le1$, the bigger $\delta(A,B)$ gets, the closer the two fuzzy sets are; the smaller $\delta(A,B)$ gets, the more distance they get.

A method for similarity degree reverse weight is presented here: choose some weights as alternative set and construct fuzzy equation for calculation solutions, and then choose the biggest one most close to the real one among the solutions, the corresponding one is what is desired. This is a heuristic method to obtain weight. The details are as followed: ***DT*** and ***RT*** obtained from formula (1) and (2) form fuzzy matrix ***R***, $R=(DT, RT)^T$; take last comprehensive trust degree as the actual evaluation B, $B=(IT, IT)^T$; design 3 possible programs: :W_1=(0.5, 0.5), W_2=(0.4, 0.6),

W_3=(0.6, 0.4); by synthetic operation get calculation evaluation $B_1=W_1 \circ R$, $B_2=W_2 \circ R$, $B_3=W_3 \circ R$; calculate similarity degree between actual evaluation and calculation evaluation, $\delta(B_1, B)$, $\delta(B_2, B)$, $\delta(B_3, B)$; choose W with the largest similarity as the similar weight.

Calculate comprehensive trust degree using the weight obtained above, the calculation formula is

$$IT_{AB} = W \bullet R \tag{3}$$

Fuzzy clustering analysis is made according to the IT matrix. The fuzzy clustering here is a method based on fuzzy equivalence relation. The specific methods are as follows: establish data matrix according to IT transposed matrix; establish similar matrix R, use Euclidean distance formula $r_{ij} = 1 - \sqrt{\sum_{k=1}^{m} (x_{ik} - x_{jk})^2}$ to define the trustee similarity of two nodes, thus, classification of trust evaluation is transferred into dynamic clustering analysis of matrices; get transitive closure $t(R)=R^*$ via square method, which is fuzzy equivalence matrix; clustering analysis can be made according to λ at different confidence levels to obtain different classification.

2.4. Malicious Node Constraint

Like defamation existing in human society, appearance of malicious nodes affects trust judgment among nodes, and firm trust established in a long time is destroyed by one or two malicious contacts. Therefore, it is necessary to introduce constraint mechanism when calculating trust value. Constraint mechanism aims at two kinds of nodes: one is neighbor nods of direct communication with direct malicious contact; the other is nodes exaggerating other malicious nodes or slandering honest nodes in the process of recommending trust. Dealing with these two kinds of nodes promptly is required to get close to actual trust.

Definition of constraint factor of the first kind of nodes:

$$\phi_{AB} = \begin{cases} 1, \left| DT_{AR} - s_{AR}^1 \right| \le 0.5 \\ 0.2, \left| DT_{AR} - s_{AR}^1 \right| > 0.5 \end{cases}$$

In this formula, ϕ_{AB} represents constraint factor of node A towards node B. If the absolute value of the difference between direct trust of node A towards node B and the latest communication record is 0.5 or less, it shows that it is within the range of being trusted; if more, it shows the possibility of malicious communication of the neighbor node. The weight of this communication record should be reduced in direct trust evaluation to eliminate adverse effects, constraint being made. If there is malicious communication in this node for a long time, the direct trust value of node A towards node B will drop rapidly providing feedback of node B in the next comprehensive trust evaluation of the whole network.

Definition of constraint factor of the second kind of nodes:

$$\phi_{iB} = \begin{cases} 1, \left| IT_{AB} - IT_{iB} \right| \le 0.5 \\ 0.2, \left| IT_{AB} - IT_{iB} \right| > 0.5 \end{cases}$$

In this formula, ϕ_{iB} represents constraint factor of node A towards node i's malicious recommendation evaluation of node B. If the difference between comprehensive evaluation of node A towards node B and that of node i towards node B is 0.5 or less , it shows that the recommendation trust value is in the range of being trusted, and this recommendation can be adopted. If more, it indicated the possibility of malicious recommendation, the weight of this recommendation in the recommendation trust evaluation is reduced. Constraint should be made to lower the adverse effects of node A towards node B in the process of recommendation trust evaluation.

3. Simulation Experiments and Results Analysis

In order to investigate the feasibility and effectiveness of subjective trust evaluation model set forth above for enterprise comprehensive evaluation, a simulation environment is configured to do simulation study and analysis. The simulation environment is PC Inter i7 2.3GHZ/2GB, Windows XP, with the code written in C.

3.1. Experiments

The node size achieved in simulation experiments is 8; the initial value of the record number of direct contact that can be stored is 3 for convenience; some other previously given initial values are: neighbor relations between nodes and direct communication record (table 1) of nodes at neighbor relations. This experiment simulated node in the network for four interactive rounds.

The neighbor relations matrix is:

$$N = \begin{Bmatrix} 0,0,1,1,0,1,0,0 \\ 0,0,0,0,1,0,1,1 \\ 1,0,0,0,1,0,0,0 \\ 1,0,0,0,1,0,0,1 \\ 0,1,1,1,0,0,0,0 \\ 1,0,0,0,0,0,1,0 \\ 0,1,0,1,0,0,0,0 \\ 0,0,0,0,0,1,0,0 \end{Bmatrix}$$

Another simulation parameter is:

σ = 0.05

Table 1 is the history record of direct contact between nodes, 0->2=(0.65, 0.6, 0.8) represents that the 3 direct contact history records of node 0 towards node 2 are (0.65, 0.6, 0.8).

Table 1. Initial Status (Direct Contact Records)

node	history records of direct contact of different nodes
0	(0→2, [0.65,0.6,0.8]) (0→3, [0.78,0.8,0.65]) (0→5, [0.65,0.5,0.85])
1	(1→4, [0.87,0.8,0.6]) (1→6, [0.88,0.8,0.45]) (1→7, [0.65,0.5,0.85])
2	(2→0, [0.67,0.8,0.91]) (2→4, [0.78,0.6,0.6])
3	(3→0, [0.89,0.9,0.75]) (3→4, [0.68,0.78,0.75]) (3→7, [0.89,0.65,0.5])
4	(4→1, [075,0.78,0.69]) (4→2, [0.88,0.85,0.75]) (4→3, [0.76,0.65,0.5])
5	(5→0, [0.82,0.6,0.62]) (5→6, [0.89,0.8,0.75])
6	(6→1, [0.91,0.85,0.65]) (6→5, [0.78,0.8,0.5])
7	(7→1, [0.9,0.78,0.66]) (7→3, [0.78,0.85,0.75])

Based on the model presented in this paper, credibility of different nodes toward target nodes is calculated and the assessment value is stored in the database. After updates of four rounds, credibility between nodes is established as is shown in table 2. After several cycles of calculating trust value, certain comprehensive credibility evaluation between nodes through recommendation trust relations is established, and the trust relation between nodes reach a stable status with the convergence rate decreasing gradually.

At this time, if node 2 intends to contact node 1, the basis on which node 1 evaluates node 1 is comprehensive evaluation towards node 1 collected from neighbor nodes (2, 3, 5).

Establish similar matrix ***R*** based on the comprehensive trust evaluation IT in the fourth round, fuzzy similar matrix can be obtained as shown in Table 3 after clustering.

Let λ =0.95, comprehensive trust evaluation is divided into 2 kinds: {1, 3}, {0, 2, 4, 5, 6, 7}.

The first comprehensive trust evaluation group: node 1, 3;

Table 2. Trust Evaluation (Initial Direct Trust Evaluation, 4th Round Comprehensive Trust Evaluation)

	0	1	2	3
0	0.00	0.00	0.70	0.74
1	0.00	0.00	0.00	0.00
2	0.78	0.00	0.00	0.00
3	0.82	0.00	0.00	0.00
4	0.00	0.74	0.80	0.67
5	0.70	0.00	0.00	0.00
6	0.00	0.78	0.00	0.00
7	0.00	0.77	0.00	0.78
	0	1	2	3
0	0.00	0.28	0.49	0.53
1	0.28	0.00	0.32	0.32
2	0.53	0.42	0.00	0.55
3	0.54	0.28	0.30	0.00
4	0.29	0.50	0.51	0.47
5	0.55	0.48	0.50	0.61
6	0.44	0.59	0.47	0.47
7	0.45	0.53	0.30	0.53

	4	5	6	7
0	0.00	0.69	0.00	0.00
1	0.75	0.00	0.72	0.69
2	0.68	0.00	0.00	0.00
3	0.74	0.00	0.00	0.69
4	0.00	0.00	0.00	0.00
5	0.00	0.00	0.79	0.00
6	0.00	0.71	0.00	0.00
7	0.00	0.00	0.00	0.00
	4	5	6	7
0	0.32	0.47	0.28	0.31
1	0.54	0.27	0.49	0.48
2	0.48	0.43	0.30	0.30
3	0.50	0.27	0.25	0.45
4	0.00	0.25	0.27	0.29
5	0.50	0.00	0.54	0.49
6	0.60	0.49	0.00	0.59
7	0.56	0.30	0.42	0.00

The second comprehensive trust evaluation group: node 0, 2, 4, 5, 6, 7.

Let λ =0.94, comprehensive trust evaluation is divided into 5 kinds: {0, 1}, {3, 7}, {4}, {2}, {5, 6}.

The first comprehensive trust evaluation group: node 0, 1;

The second comprehensive trust evaluation group: node 3, 7;

The third comprehensive trust evaluation group: node 4;

The fourth comprehensive trust evaluation group: node 2;

The fifth comprehensive trust evaluation group: node 5, 6.

Therefore, nodes 0, node 1 and node 3 are similarly evaluated in comprehensive trust evaluation, and

Table 3. Fuzzy Equivalence Matrix

	0	1	2	3
0	1.00	0.94	0.94	0.94
1	0.94	1.00	0.94	0.95
2	0.94	0.94	1.00	0.94
3	0.94	0.95	0.94	1.00
4	0.94	0.94	0.93	0.93
5	0.93	0.93	0.93	0.93
6	0.93	0.93	0.93	0.93
7	0.94	0.94	0.94	0.93

	4	5	6	7
0	0.94	0.93	0.93	0.94
1	0.94	0.93	0.93	0.94
2	0.93	0.93	0.93	0.94
3	0.93	0.93	0.93	0.93
4	1.00	0.93	0.93	0.94
5	0.93	1.00	0.93	0.93
6	0.93	0.93	1.00	0.93
7	0.94	0.93	0.93	1.00

the evaluation results of the other five nodes are similar, which is close to actual situation. Fuzzy clustering analysis reflects the approximate distribution of eight nodes in comprehensive trust evaluation, which helps one node understand credibility of other nodes and make decisions.

3.2. Malicious Recommendation Experiments and Results Analysis

To test whether this model can shield effectively malicious recommendation messages, we suppose that node 3 is a malicious node, providing malicious recommendation DT_{34}. Suppose the value is 0.2, after one round's update as shown in Table 4, we find that DT_{03} dropped immediately from 0.74 to 0.26 and all direct trust evaluation towards node 3 reduced greatly. However, there are some drawbacks, i.e. like in human society, when you don't trust one person, you are not likely to contact his or her friends. The entire network is interconnected and mistrust caused by such malicious recommendation can spread to the entire network. The positive side is that this model can constrain malicious nodes quickly and to a certain degree avoid mistrust towards other nodes caused by malicious recommendation.

Figure 2 shows the change in comprehensive credibility of IT_{03} in a period of time. As is shown in Table 2, as the value of constraint factor is 0.2, 0.6 and none, credibility vary with changes in constraint factor. The smaller the value of constraint factor is, the more obvious the constraints are to minimize the adverse effects of malicious evaluation caused by malicious nodes. The 3 comprehensive trust value would converge to a fixed value.

Table 4. the 5th Round Direct Trust Evaluation with Malicious Nodes

	0	1	2	3
0	0.00	0.00	0.30	0.26
1	0.00	0.00	0.00	0.00
2	0.27	0.00	0.00	0.00
3	0.29	0.00	0.00	0.00
4	0.00	0.26	0.28	0.29
5	0.30	0.00	0.00	0.00
6	0.00	0.27	0.00	0.00
7	0.00	0.27	0.00	0.27

	4	5	6	7
0	0.00	0.29	0.00	0.00
1	0.26	0.00	0.25	0.29
2	0.29	0.00	0.00	0.00
3	0.26	0.00	0.00	0.29
4	0.00	0.00	0.00	0.00
5	0.00	0.00	0.28	0.00
6	0.00	0.25	0.00	0.00
7	0.00	0.00	0.00	0.00

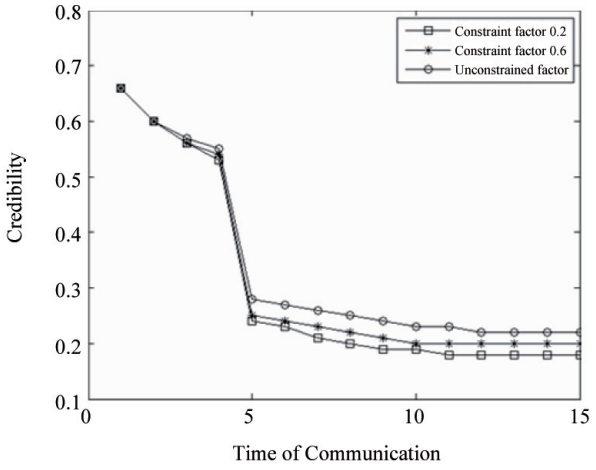

Figure 2. Change of Credibility with Change in Time of Communication

3.3. Analysis of Trust Computing Accuracy

The purpose of this experiment is to test the evaluation accuracy of the subjective trust evaluation model presented above in evaluation between nodes when fuzzy theory is introduced, compared with the evaluation model mentioned in literature 9. Table 5 is the comparison of trust evaluation data after algorithm processing. Weighted Hamming distance analysis is adopted to decide which one of the two models mentioned in literature 9 and the proposed one in this paper is closer to the ideal evaluation.

Let Universe U={u_1(trust evaluation of node 0 towards node 2), u_2(trust evaluation of node 0 towards node 3), u_3(trust evaluation of node 0 towards node 1)}, A be model in literature 9 after algorithm processing, B be model presented in this paper, C be the fuzzy set of these models.

$\underline{A}=0.53/u_1+0.60/u_2+0.65/u_3$

$\underline{B}=0.49/u_1+0.53/u_2+0.28/u_3$

$\underline{C}=0.41/u_1+0.50/u_2+0.44/u_3$

Weighted W=(0.2, 0.3, 0.5)

Weighted Hamming distance

$d(\underline{A},\underline{C})=0.2*0.12+0.3*0.1+0.5*0.21=0.159$

$d(\underline{B},\underline{C})=0.2*0.08+0.3*0.03+0.5*0.16=0.105$

It shows that $d(\underline{A},\underline{C})> d(\underline{B},\underline{C})$, indicating that model presented in this paper is much closer to ideal evaluation compared with that mentioned in literature 9. Therefore, subjective trust evaluation model presented in this paper with fuzzy theory introduced is more suitable to evaluate nodes in network environment than that mentioned in literature 9.

Table 5. Comparison of trust evaluation models

Nodes model	mentioned in literature 9	model presented in this paper	ideal evaluation
0->2	0.53	0.49	0.41
0->3	0.60	0.53	0.50
0->1	0.65	0.28	0.44

Conclusions

This paper presents a comprehensive trust evaluation model based on fuzzy theory, puts forward direct trust evaluation, recommendation trust evaluation and comprehensive trust evaluation, refines credibility obtained through different methods, tests the feasibility and effectiveness of this subjective trust evaluation model on enterprise comprehensive evaluation via simulation experiments, improves the accuracy and rapidity of trust evaluation model on assessing credibility and makes this model adapt to open network environment better.

References

1. Wenhua Huang, Yishuang Geng, Identification Method of Attack Path Based on Immune Intrusion Detection, Journal of Networks, 2014,9,pp. 964-971.
2. Guanqun Bao, Liang Mi, Yishuang Geng, Mingda Zhou, Kaveh Pahlavan, A video-based speed estimation technique for localizing the wireless capsule endoscope inside gastrointestinal tract, 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Sydney, 2014,pp.1298-1302.
3. Degui Zeng, Yishuang Geng, Content distribution mechanism in mobile P2P network, Journal of Networks, 2014,9,pp. 1229-1236.
4. Mingda Zhou, Guanqun Bao, Yishuang Geng, Bader Alkandari, Xiaoxi Li, Polyp detection and radius measurement in small intestine using video capsule endoscopy, 2014 7th International Conference on Biomedical Engineering and Informatics (BMEI), London,2014,pp.365-368.
5. Gan Yan, Yuxiang Lv, Qiyin Wang, Yishuang Geng, Routing algorithm based on delay rate in wireless cognitive radio network, Journal of Networks, 2014,9, pp.948-955.
6. Guanqun Bao, Liang Mi, Yishuang Geng, Kaveh Pahlavan, A computer vision based speed estimation technique for localiz ing the wireless capsule endoscope inside small intestine, 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), New York, 2014, pp.89-99.
7. Xinchao Song, Yishuang Geng, Distributed community detection optimization algorithm for complex networks, Journal of Networks, 2014,10, pp.2758-2765.
8. Dingde Jiang, Zhengzheng Xu, Peng Zhang, and Ting Zhu. A transform domain-based anomaly detection approach to network-wide traffic.Journal of Network and Computer Applications , 2014,40,pp.292-306.
9. Xiaoming Li, Zhihan Lv, Baoyun Zhang, Weixi Wang, Shengzhong Feng, Jinxing Hu. XEarth: A 3D GIS Platform for managing massive city information. 2015 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications(CIVEMSA), Sydney, 2015, pp. 356-368.
10. Liguo Zhang, Binghang He, Jianguo Sun, Mingzhu Lai, Zhihan Lv. Double Image Multi-Encryption Algorithm based on Fractional Chaotic Time Series. Journal of Computational and Theoretical Nanoscience. 2015,4,pp.412-415.
11. Wei Luo, Zhiyong Wang, Zhihan LV. Method to Acquire a Complete Road Network in High-resolution Remote Sensing Image Based on Tensor Voting Algorithm. EXCLI JOURNAL,2015,4,pp.44-48.
12. Song Zhang, and Huajiong Jing. Fast log-Gabor-based nonlocal means image denoising methods. 2014 IEEE International Conference on Image Processing (ICIP). Beijing, 2014, pp. 2724-2728.
13. Jiachen, Yang, et al.. Wang H; Multiview image rectification algorithm for parallel camera

arrays. J. Electron. Imaging. 2011;23,pp.103-110.
14. Alex Tek, et al.. Advances in Human-Protein Interaction-Interactive and Immersive Molecular Simulations." Biochemistry, Genetics and Molecular Biology.Protein-Protein Interactions-Computational and Experimental Tools. 2012,12,pp.27-65.
15. Zhihan Lv, Alaa Halawani, Shengzhong Feng, Shafiq ur Rehman, Haibo Li. Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device. Personal and Ubiquitous Computing. 2015,5,pp.123-125.

Research of a Mixed Robust H_2 / H_∞ Controller Design for NCS with Variable Sampling Intervals and Time-delay

Yan-guang Li[1], Hao Bu[2]

1College of Mathematics and Computer Application, Shangluo University, Shangluo Shanxi , 726000, China
2College of Urban,Rural Planning and Architetural Engineering, Shangluo University, Shangluo Shanxi , 726000, China

Corresponding author is Yan-guang Li

Abstract
Based on Lyapunov stability theory and linear matrix inequalities (LMIs) method, parameter-dependent and parameter-independent states feedback controller, the states feedback controller and dynamic output feedback controller are designed, respectively. The necessary and sufficient condition of existence the above controllers are given by LMIs. Considering the disturbance and noise, the mixed robust H_2 / H_∞ performance of the discrete-time polytopic uncertain system is proposed, which is used to improve the system transient performance and to ensure the robustness of the system simultaneously. Finally, the robust states feedback and dynamic output feedback controllers are designed and an example is given to show its effectiveness.
Key words: LYAPUNOV; LMIS; H_2 / H_∞; ROBUST CONTROL

1. Introduction

NCSs(Networked Control Systems) are some feedback control systems where the feedback loops are closed by some communication networks. NCSs have many advantages such as less wiring, easy installation and maintenance, etc. In recent years, there are many research about NCSs. There are also many special issues for NCSs published by some International Journals[1-6]. In the practical network control system, stability and controller design will be impact-