International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 123-132
http://dx.doi.org/10.14257/ijsia.2015.9.5.13

A Multi-dimensional Evidence-based Trust Evaluation Model and Algorithm

Wenbao Jiang[1], Qijing Li[2] and Wenliang Chen[2]

School of Information Management, Beijing Information Science &Technology University, Beijing, China
jiangwenbao@tsinghua.org.cn, wonderlandli@163.com, yeacheng5@gmail.com

Abstract

Trust evaluation is increasingly important for collaboration in the Internet today. We propose a multi-dimensional evidence-Based trust evaluation model named EBTrust model, which expands the types and sources of evidence. We put both transaction feedback and the network operating behavior information into this model. And we improve the D-S evidence theory and propose a new rule of evidence synthesis that based on the conflict intensity (G) and efficient conflict (Gh), so we call it G-Gh synthesis rule, which can not only solve the high confliction and complete conflict feature of multi-dimensional evidences but also the problem of uncertainty in the process of trust evaluation. The example analysis and experimental results show that the EBTrust model can resist conspiracy and malicious comment behavior.

Keywords: *trust management, D-S evidence theory, synthesis rule, multi-dimensional evidence*

1. Introduction

Trust Management is presented as a new security mechanism for all open and distributed environments, and trust evaluation is one of the most important issues in Trust Management. There is a demand for trust evaluation from P2P networks, e-commerce applications, service oriented computing and multi-agent systems, in which it is important to evaluate the trustworthiness of participating entities since trust is the major driving force for collaboration.

Currently, there are some models and methods of trust evaluation. Yu [1] proposes that local experience (local evidence) and the assessment from other nodes are both to be considered, he used the D-S evidence theory to spread and merge the trust evaluation from an agent to other agents. Luolai Yuan and Guosun Zeng [2] propose a trust evaluation model based on transaction feedback and the original D-S evidence theory. In order to solve the problem of the synthesis rules and confliction information in the actual application of D-S evidence theory, Matsuyama [3], Yager [4], Xiaoxia Wang [6] and Murphy [5] have done some researches on the evidence synthesis and put forward their own improvement method.

This paper proposes a multi-dimensional evidence based trust evaluation model called EBTrust model. We use multi-dimensional evidence to expand the types of evidence and the sources of evidence, meanwhile we improved D-S evidence synthesis rule and propose a G-Gh synthesis rule to synthesize the multi-dimensional evidence, which can solve the problem of uncertainty better in the process of trust evaluation.

The rest of the paper is organized as follows. Firstly, we describe the framework of EBTrust model in Section 2. Then we introduce Evidence preprocessing in Section 3. Further, Section 4 gives the construction of basic trust function, and Section 5 elaborates G-Gh synthesis algorithm. We provide experiment and analysis in Section 6. Finally, the conclusions are drawn in Section 7.

ISSN: 1738-9984 IJSIA

2. Framework of EBTrust Model

EBTrust is a new trust evaluation model based on multi-dimensional evidence and G-Gh evidence synthesis rule, which not only expands the types of evidence and evidence sources, but also solves the problem of uncertainty better in the process of trust evaluation. The Figure 1 shows the structure of EBTrust model.

In this paper, the design of EBTrust model is similar to a centralized trust model. This model is dividing into three main modules: the evidence collection module, evidence formal processing module and trust calculation and management module.

Figure 1. Framework of EBtrust Model

Evidence collection module collect the multi-dimensional evidence mainly, this multi-dimensional evidence includes three Sections: e-commerce feedback, online community feedback and network operating behavior feedback.

Evidence formal processing module is responsible to process the original evidence that have various forms and complex structure in order to achieve a formal expression. This module will be dividing into two small modules. One is evidence preprocessing, which is process three types of evidence and construct data structure. The other is structure basic trust function module, which constructs three types of evidence's trust function.

Trust calculation and management module responsible to the final calculation of trust, as well as to store, update, retrieve and release the data of trust degree. It contains G-Gh evidence synthesis center and the trust degree management center.

3. Evidence Preprocessing

The original evidences from the evidence collection module are expressed as natural language or other non-mathematical language, and the same type of evidence from different sources of evidence may have different complex structures. So it is important to preprocessing the original evidence.

The existing trust evaluation mainly includes trading volume, trading volume, transaction time, transaction results and transaction evaluation etc.. But most of these evidences can be classified as business feedback based evidence. These evidences have obvious limitations. It ignores the impact of network operating activities related to transactions to transactions. And it only considers the performance of the subject in a specific type of transaction.

In view of the above limitations, we put forward the concept of multidimensional evidence to evaluate the subject of network reliability. Multidimensional refers to the different types of evidence. Multidimensional evidence involved in our proposed model

including electronic commerce feedback evidence, the community network service feedback evidence, network operation behavior evidence.

3.1 Preprocessing of E-commerce Feedback Evidence

The data structure of e-commerce feedback evidence after preprocessing can be described as: Evi (Cla, Ide, T, Val, Res, Asse), and we defined:

- Cla is the variable of the type of evidence and the value is 1.
- Ide is the variable of network subjective identity, and $Ide \in \{-1,1\}$, Ide=1 shows that the current subject is the seller, Ide=-1 shows that the current subject is buyer.
- The time variable T is equal to the time of the current evidence, that means the current online transaction occurred time.
- Val is the variable of the transaction value, Val equal to the value of the transaction of the current evidence, measured in monetary currency.
- Res is the variable of the result of transaction, Res=-1 indicate that the responsibility for itself when the current transaction is failed. Res=0 indicates that the responsibility for other side when the current transaction is failed. Res=1 indicates that the current transaction complete successfully.
- The variable of transaction evaluation and Asse=-1 shows that the other side give a negative assessment to own side. Asse=0 shows that the other side give a medium evaluation or fails to make an assessment. Aesse=1 shows that the other side made a positive assessment.

3.2 Preprocessing of Online Community Feedback Evidence

The data structure of online community feedback evidence after preprocessing can be described as: Evi (Cla, Eve, T, Disti), the variable of it will define as:

- Cla is the variable of the type of evidence and the value is 2.
- Eve is the variable of event, Eve=1 shows that the home page that the current evidence point to was browsed. Eve=2 shows that the original posts were browsed. Eve=3 shows that the posts were deleted by administrator. Eve=4 shows that the posts were prohibited by the administrator.
- The time variable T is the time of the current evidence accrues.
- Disti is the variable of the event judgment, the value of Disti associated with the variable of event Eve, so the specific value will be showed in Table .

Table 1. The Specific Value of Disti

Eve	Disti
1	The times of browsed
2	The times of browsed
3	Disti=1, the object is poster. Disti=-1, the object is commentator
4	Disti=1, the object was temporarily prohibited posting. Disti=-1 the object was permanently prohibited posting or delete the id of object.

3.3 Preprocessing of Operating Behavior Feedback Evidence

The data structure of operating behavior feedback evidence after preprocessing can be described as: Evi (Cla, T, Lev), and the variable will describe as:

- Cla is the variable of the type of evidence and the value is 3.
- The time variable T is the time of the current evidence behavior accrues.
- Lev is the level of act endangers (or attack level), the classification of the attack level will be shown in Table 2.

Table 2. The Attack Level

Attack level	The type of attack	Attack listed
1	Information disclosure	Read files, memory data, registry, port and so on.
2	Refuse service	Cpu consumption, memory consumption, decreased quality of service, disk space consumption and so on.
3	Data destruction and deception	Tampered with the file system, memory data, system kernel, database configuration and so on.
4	Intrusion control	Illegal execution, unauthorized access to the file system, illegal acquisition of shell and so on.
5	Antagonistic	Bypass virus detection, penetrate the firewall, communication hidden functions and so on

4. Construction of Basic Trust Function

For any subject of one network, it is assumed that the evidence is sufficient, so determine its trust only have two cases: trust and distrust. Therefore we can construct the identification framework: , it can abbreviated as: $\Theta = \{t, d\}$,

So, $2^{\Theta} = \{\phi, \{t\}, \{d\}, \Theta\}$.

Then possible focus elements of Θ are {t}、{d}、Θ, this paper will represent these focus element as proposition T、D、Θ, so $T = \{t\}$, $D = \{d\}$, Θ

Therefore, we construct the basic trust distribution function in the form of: $m(T, D, \Theta)$

We assume that a network subject A. when construct a basic trust function of e-commerce feedback evidence, we consider the results and the effect of evaluation of the actual e-commerce and constructs a basic trust function of feedback evidence. Whatever the network subject A is seller or buyer, the specific structure of a basic trust function of feedback evidence can be shown in Table III. When construct a basic trust function of online community feedback evidence, we also consider the effect of behavior of subject on the trust, so the trust function of online community feedback can be describe as Table IV. We construct the basic trust function of operating behavior feedback evidence based on the effect of operate behavior on the subject A, so the trust function of operating behavior feedback can be describe as Table V.

Table 3. The Trust Function of E-Commerce Feedback Evidence

Id	$Evi(Cla, Tde, T, Val, Res, Asse)$	$m(T, D, \Theta)$	Instruction
1	$(1, Tde, T, Val, 1, 1)$	$(1, 0, 0)$	Transaction is successfully, and get a positive assessment, so A is trusted
2	$(1, Tde, T, Val, 1, 0)$	$(0.5, 0, 0.5)$	Transaction is successfully, and gets a medium assessment or missing assessment, so A is not completely trusted.
3	$(1, Tde, T, Val, 1, -1)$	$(0, 1, 0)$	Transaction is successfully, and gets a negative evaluation, so A is distrust.
4	$(1, Tde, T, Val, 0, 1)$	$(0.5, 0, 0.5)$	Transaction failed because of the problem of other side and gets a positive assessment, so A is not completely trusted.
5	$(1, Tde, T, Val, 0, 0)$	$(0, 0, 1)$	Transaction failed because of the problem of other side and gets a medium assessment or missing assessment, so we can't judge A trust

			or not.
6	$(1, Tde, T, Val, 0, -1)$	$(0,1,0)$	Transaction failed because of the problem of other side and gets a negative evaluation, so A is distrust.
7	$(1, Tde, T, Val, -1, 1)$	$(0.5, 0, 0.5)$	Transaction failed because of the problem of A and gets a positive evaluation, so A is not completely trusted.
8	$(1, Tde, T, Val, -1, 0)$	$(0, 0.5, 0.5)$	Transaction failed because of the problem of A and gets a medium assessment or missing assessment, so A is not completely distrusted.
9	$(1, Tde, T, Val, -1, -1)$	$(0,1,0)$	Transaction failed because of the problem of A and gets a negative evaluation, so A is distrust.

Table 4. The Trust Function of Online Community Feedback Evidence

Id	$Evi(Cla, Eve, T, Disti)$	$m(T, D, \Theta)$	Instruction
1	$(2,1,T, Disti)$	$(1,0,0)$	The home page of A was browsed, so A is trust.
2	$(2,2,T, Disti)$	$(1,0,0)$	A post was browsed, so A is trust.
3	$(2,3,T, Disti)$	$(0,1,0)$	A post was deleted by administrator, so A is distrust.
4	$(2,4,T, Disti)$	$(0,1,0)$	Subject A has disabled a post, so A is distrust.

Table 5. The Trust Function of Operating Behavior Feedback Evidence

Id	$Evi(Cla, T, Lev)$	$m(T, D, \Theta)$	Instruction
1	$(3, T, Lev)$	$(0,1,0)$	Network operating behavior has produced, that means A makes the danger operating behavior, so A is distrust.

5. G-Gh Synthesis Algorithm

The main task of the G-Gh evidence synthesis is the calculation of trust. In the practical application process, there are usually many evidence of a proposition or proposition set effect. Different evidence may have different basic distribution function. In order to calculate the trust function and plausibility function, first of all the different basic belief assignment function are combined into a probability distribution function. Dempster proposed a method for the synthesis of different basic belief assignment function, a combination rule of D-S evidence. Due to the multi-dimensional evidence has high confliction feature and even there are some complete conflict evidence, so the existence of D-S synthesis rules and the improvement synthesis rules that Smets [8], Yager [4], Lefevre [9] proposed are not available. So we proposed a new rule of evidence synthesis that based on the conflict intensity (G) and efficient conflict (Gh), so we call it G-Gh synthesis rule. The step of this synthesis rules as follows:

- Based on conflict intensity G, all evidence of trust collation value weighted average.
- Use of efficient conflict synthesis method to synthesized $m\left(A_i^e\right)$ n-1 times and the number of $m\left(A_i^e\right)$ is n.

The G-Gh synthesis rules will be specifically describe as: assume that m_1, m_2, ….., m_n is the basic trust allocation function of evidence E1, E2, …, En of the discernment frame Θ. A_1, A_2, …, A_l are all focal elements of all the evidence, so the G-Gh synthesis rules are as follows.

5.1 Conflict intensity G

The literature [7] gives the definition of conflict intensity G: assume that m_1 , m_2 are the basic trust allocation function of evidence E_1, E_2 of the discernment frame Θ . The focal element is A_{1i}、 A_{2j}, so

$$\begin{cases} G(E_1,E_2)=\dfrac{C(E_1,E_2)}{H(E_1,E_2)+C(E_1,E_2)} \\ C(E_1,E_2)=\sum\limits_{A_{1i}\cap A_{2j}=\varnothing} m(A_{1i})m(A_{2j}) \\ H(E_1,E_2)=\sum\limits_{A_{1i}=A_{2j}} m(A_{1i})m(A_{2j}) \end{cases} \quad (5\text{-}1)$$

5.2 Weighted Average the Value of the Trust Allocation

For any two evidence E_i、 E_j, we defined $b_{ij}=1-G_{ij}=b_{ji}$ as the similarity of evidence E_i、 E_j, and $b_{ii}=b_{jj}=1$, so we can obtain the similarity matrix of all evidence, the number of evidence is n.

$$s=\begin{pmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{i1} & \cdots & b_{ij} & \cdots & b_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nj} & \cdots & b_{nn} \end{pmatrix}=\begin{pmatrix} 1 & \cdots & b_{1j} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{i1} & \cdots & 1 & \cdots & b_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nj} & \cdots & 1 \end{pmatrix} \quad (5\text{-}2)$$

The smaller conflict intensity between the evidence, the greater the intensity of the evidence to support each other, so the sum of each line element of the matrix S is the support intensity of all other evidence on E_i.

$$Sup(m_i)=\sum_{j=1}^{n} b_{ij}, (\mathrm{i,j=1,2,\ldots,\ n}) \quad (5\text{-}3)$$

We can get the weight of the weighted average from the normalization of support intensity.

$$Weit(m_i)=Sup(m_i)\Big/\sum_{i=1}^{n} Sup(m_i), (\mathrm{i,j=1,2,\ldots,\ n}) \quad (5\text{-}4)$$

At this point, the number of n groups of evidence of basic trust collation value weighted average.

$$m(A_l^e)=\sum_{i=1}^{n} Weit(m_i)m_i(A_l) \quad (5\text{-}5)$$

5.3 Efficient Conflict G_h

We can obtain a basic trust allocation function after weighted average through the above steps.

$m^e(A)=m^e(\{A_1\},\{A_2\},\ldots\{A_l\})=(m^e(A_1),m^e(A_2),\ldots,m^e(A_n))$

We divide the conflict part into two parts of the efficient conflict and inefficient conflict in this article. Efficient conflict refers to the efficient part in the process of the proposition discrimination and the inefficient conflict is the inefficient part in the process of the proposition discrimination. Reference the definition of the amount of consistent and the amount of conflict of the evidence to the literature [7], so we defined the efficient part of the conflict as:

m_1 , m_2 are the basic trust allocation function of evidence E1, E2 of the discernment frame Θ. The focal element is A_{1i}、 A_{2j}, A_1, A_2, …, A_l are all focal elements of all the evidence.

Definition 1 the amount of consistent of E1 and E2:

$$H(E_1,E_2)=\sum_{A_{1i}=A_{2j}} m(A_{1i})m(A_{2j}) \quad (5\text{-}6)$$

Definition 2 the amount of conflict of E1 and E2:

$$C(E_1,E_2)=\sum_{A_{1i}\cap A_{2j}=\varnothing} m(A_{1i})m(A_{2j}) \quad (5\text{-}7)$$

Definition 3 efficient conflicts of E1 and E2:

$$G_h(E_1,E_2)=\frac{H(E_1,E_2)}{H(E_1,E_2)+C(E_1,E_2)} \quad (5\text{-}8)$$

Based on these definitions, efficient conflict synthesis can be described as:

$$m(A_i)=\begin{cases}\sum_{A_{1i}\cap A_{2j}=A_i} m_1(A_{1i})m_2(A_{2j})+\Delta\varphi * G_h * K, A\neq\Theta \\ \sum_{A_{1i}\cap A_{2j}=A_i} m_1(A_{1i})m_2(A_{2j})+(1-G_h)*K, A=\Theta\end{cases} \quad (5\text{-}9)$$

Where $\Delta\varphi=\begin{cases}\frac{m_1(A_i)+m_2(A_i)}{\sum m_1(A_{1i})m_2(A_{2j})} & , A_i, A_{1i}, A_{2j} aren't \text{ focal elements of } \Theta \\ 0 & , A_i=\Theta\end{cases}$

5.4 Algorithm of G-Gh

G-Gh synthesis rule retains the commutative law and the associative law of the D-S synthetic. This article design a new algorithm of synthesized $m(A_i^e)$ n-1 times and the number of $m(A_i^e)$ is n. the algorithm as follows:

$m_0^e(A)\leftarrow m^e(A)$
$m(A)\leftarrow m_0^e(A)$
$l\leftarrow n$
$m\leftarrow n-1$
$flag_{m-1}\leftarrow 0$
while $l>1$
  do $m_m^e(A)\leftarrow m_{m-1}^e(A)\oplus m_{m-1}^e(A)$
    $flag_m\leftarrow l\%2$
    $l\leftarrow int(l/2)$
    if $flag_{m-1}=1$
      then $m(A)\leftarrow m(A)\oplus m_{m-1}^e(A)$
end
$m(A)\leftarrow m(A)\oplus m_m^e(A)$

6. Experiment and Analysis

6.1 Resistance of Conspiracy Behavior

Existing trust evaluation model is the lack of effective measures to resist conspiracy, so some person increases the trust of each other by the conspiracy behavior. The model that this paper designed makes the cost of achieves the desired results increase greatly, therefore reducing the conspiracy behavior. Set within the time window t, the system collect the evidence on the subject A within the time window t, the evidence contains two e-commerce feedback evidence, one network community feedback evidence, one network operating behavior evidence. The structure of these evidences are: Evi1(1, 1, t, 500, 1, 1), Evi2(1, 1, t, 1500, 1, 1), Evi3 (2, 1, t, 12000), Evi4 (3, t, 1). The result of trust evaluation by G-Gh synthesis rule is (0.0566, 0.1091). Assume the subject A want enhance itself trust value by conspiracy behavior, his method is online sale of goods worth 500yuan, and looking for conspiracy partner to buy the goods. The paid and the results obtain shows in Figure 2.

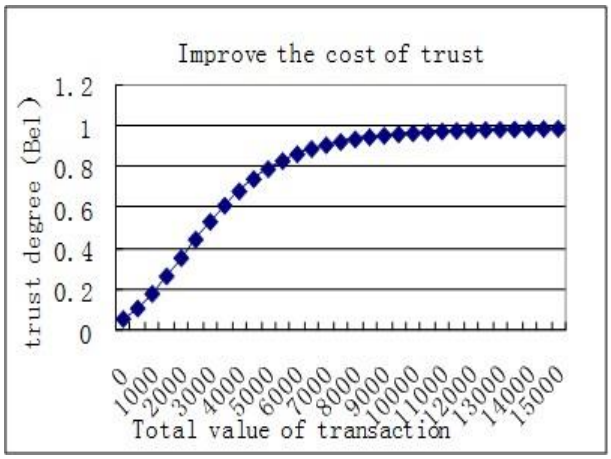

Figure 2. Improve the Cost of Trust

We select a few important points to examine the size of the overhead. By the graph, the cost of trust is 3500yuan, 4500yuan, 5500yuan, 7000yuan and 8500yuan when improve the trust degree to 0.6, 0.7, 0.8, 0.9, 0.95. So, the cost of achieves the desired trust increase greatly, which can reduce the impact of conspiracy for the trust evaluation.

6.2 Resistance of Malicious Comment Behavior

There is a subject A produces the trust distribution functions within the time window t, shown in Figure 3, the trust is (1.0, 1.0). Subject B want reduce the trust of subject A through a malicious assessment. Assume that subject A only sell the price of 500yuan of goods, then the cost of subject B to reduce the subject A's trust shown in Figure 4.

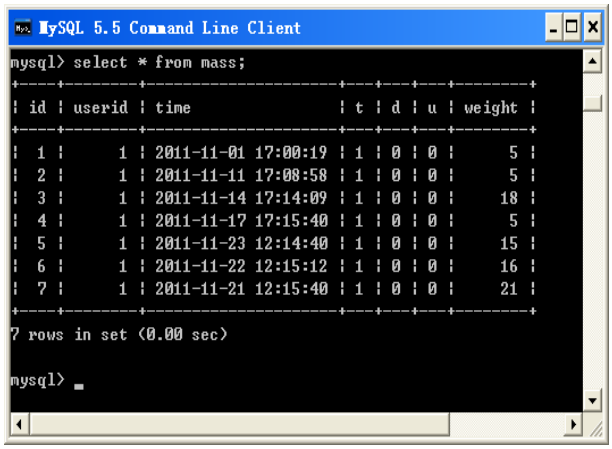

Figure 3. Trust Distribution Function of Subject A

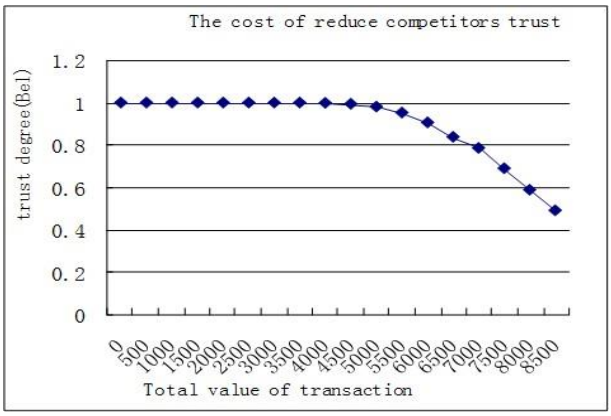

Figure 4. The Trust Cost Trend of Competitors

The trust degree of subject A will below value of 1 when transaction with subject B ten times. But the cost of B is 5000yuan. If B continues to give malicious comment, the trust degree of A continue decline. When complete the15th transaction, the trust degree of A is 0.5, but the cost of B is 8500yuan. So the cost of B increase quickly when he wants reduces the trust degree of A through the malicious comment. When A observes B's malicious behavior, he can refuse to continue to transaction with B, which can effectively reduce the impact of trust evaluation.

7. Conclusions

Although many trust evaluation models have previously been proposed, precise security goals and properties are lacking. In this paper, we analyze and design an EBtrust model which is based on multi-dimensional evidence. We expanded the types of evidence and evidence sources and improved the D-S evidence synthesis rules, analyzed and designed a G-Gh synthesis rules. All the work makes EBtrust model can solves the problem of uncertainty in the process of trust evaluation.

The theoretical analysis and test results reveal that EBtrust model has high efficiency on Resistance of collusion behavior and malicious evaluation behavior. The work of this paper will contribute strong theoretical and academic significance to the trust evaluation.

EBtrust model is the expansion of NBTEM (network behavior based trust evaluation model) [10] proposed by our group in 2010. This model didn't deep study in the collection of evidence and the evidence synthesis rule not very satisfied, which need study in the future work.

Acknowledgments

This work is financially supported by The National Natural Science Foundation of China (60873202) and Beijing Natural Science Foundation (4132011)

References

[1] Y. Bin and M. P. Singh, "An evidential model of distributed reputation management", Proc. of the 1st International Joint Conference on Autonomous Agents and Multi-agent Systems, New York: ACM Press, **(2002)**, pp. 294-301.
[2] L. Yuan and G. Zeng, Trust evaluation model based on Dempster-Shafer theory of evidence", Wuhan University(Natural Science Edition), vol. 52, no. 5, **(2007)**, pp. 627-630.
[3] T. Matsuyama, "Belief Formation Observation and Belief Integration Using Virtual Belief Space in Dempster-Shafer Probability Model", Proc. of the 1994 IEEE on Multi-sensor Fusion and Integrating for Intelligent System. Los Vegas, NV, **(1994)**, pp. 379-386.
[4] R. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules", IEEE Trans. on System, vol. 41, no. 2, **(1989)**, pp. 93-137.

[5] C. K. Murphy, "Combining Belief Functions when Evidence Conflicts", Decision Support System, vol. 29, no. 1, **(2000)**, pp. 1-9.
[6] X. Wang and F. Yang, "A deal with conflict of evidence synthesis method", Missiles and guidance, vol. 27, no. 5, **(2007)**, pp. 255-257.
[7] F. Yang and Xiaoxia, "The conflict evidence synthesis method of D-S evidence theory", Beijing: National Defence Industry Press, vol. 2, **(2010)**, pp. 2-3.
[8] P. Smets, "The Combination of Evidence in the Transferable Belief Model", IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 12, no. 5, **(1990)**, pp. 447-458.
[9] E. Lefevre, O. Clot, *et al.*, "A Generic Framework for resolving the conflict in the combination of belief structures", The 3rd International Conference on Information Fusion, vol. 1998, **(2000)**, pp. 182-188.
[10] W. Jiang, S. Guo and W. Chen, "A Trust Evaluation Model and Algorithm Based on Network Behavior Detection", Beijing: IEEE, IC-BNMT, **(2010)**.

Authors

Wenbao Jiang, received his Ph.D. degree in information security from Graduate University of Chinese Academy of Sciences in 2003. He was a postdoctoral researcher in the Department of Computer Science and Technology at Tsinghua University from 2003-2005. He is currently an associate professor and vice dean of School of Information Management, Beijing Information Science & Technology University. His major research interests include network security, trust management, trust negotiation.

Qijing Li, received her bachelor of management from Tangshan Normal Univercity, Tangshan, Hebei, China, 2012. She is currently a Master degree candidate in Information Science & Technology University, Beijing, China. Her research interests including information security.

Wenliang Chen, received his bachelor of management from Information Science & Technology University, and Master of management degree in Management Science and Engineering from Information Science & Technology University, Beijing, China, in 2009 and 2012, respectively. His research interests focus on information security.

