Sensors **2011**, *11*, 1345-1360; doi:10.3390/s110201345

OPEN ACCESS

sensors

ISSN 1424-8220

www.mdpi.com/journal/sensors

Article

A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory

Renjian Feng *, Xiaofeng Xu, Xiang Zhou and Jiangwen Wan

School of Instrument Science and Opto-electronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191, China; E-Mails: alickelly@gmail.com (X.X.); zhouxiangbuaa@163.com (X.Z.); sensory@buaa.edu.cn (J.W.)

* Author to whom correspondence should be addressed; E-Mail: rjfeng@buaa.edu.cn; Tel.: +86-10-8233-8089; Fax: +86-10-8233-9889.

Received: 9 December 2010; in revised form: 27 December 2010 / Accepted: 18 January 2011 / Published: 25 January 2011

Abstract: For wireless sensor networks (WSNs), many factors, such as mutual interference of wireless links, battlefield applications and nodes exposed to the environment without good physical protection, result in the sensor nodes being more vulnerable to be attacked and compromised. In order to address this network security problem, a novel trust evaluation algorithm defined as NBBTE (Node Behavioral Strategies Banding Belief Theory of the Trust Evaluation Algorithm) is proposed, which integrates the approach of nodes behavioral strategies and modified evidence theory. According to the behaviors of sensor nodes, a variety of trust factors and coefficients related to the network application are established to obtain direct and indirect trust values through calculating weighted average of trust factors. Meanwhile, the fuzzy set method is applied to form the basic input vector of evidence. On this basis, the evidence difference is calculated between the indirect and direct trust values, which link the revised D-S evidence combination rule to finally synthesize integrated trust value of nodes. The simulation results show that NBBTE can effectively identify malicious nodes and reflects the characteristic of trust value that 'hard to acquire and easy to lose'. Furthermore, it is obvious that the proposed scheme has an outstanding advantage in terms of illustrating the real contribution of different nodes to trust evaluation.

Keywords: wireless sensor networks; network security; trust evaluation; node behaviors; evidence theory

---

1. Introduction

Recent technology development in the fields of wireless communication and MEMS has facilitated the extensive distribution of wireless sensor networks (WSNs) which are reliable, accurate, flexible, inexpensive and easy to deploy. In many applications, for instance, environment monitoring and battlefield spying, the nodes are vulnerable to be attacked by passive eavesdropping, active intrusion, message flooding, fake information inserting, *etc*. Among the above hostile attacks, passive eavesdropping helps adversaries intercept private information. Active intrusion makes it possible for adversaries to delete information, insert false information or impersonate nodes, which destroy the usability, integrality, security certificate and non-reputation of WSNs. Unfortunately, the available complicated encryption algorithms are unsuitable for WSNs because of the restricted capabilities of low cost nodes. Hence, the WSNs usually adopt security method based on symmetric cryptographic methods.

However, the intrusion detection and prevention schemes with cryptographic protection are unable to identify the destructive threat by the authenticated nodes which have been compromised. If the compromised nodes cannot be identified in time, secret information may be revealed and the whole network could be under the control of the adversaries. Therefore, an efficient mechanism is urgently needed to identify the compromised nodes and take measures to minimize the destruction or loss in the network.

Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. It has been widely studied in many network environments such as peer-to-peer networks, grid and pervasive computing and so on. However, in reality, sensor nodes have limited resources and other special characters, which make trust management for WSNs more significant and challenging. Up to the present, research on the trust management mechanisms of WSNs have mainly focused on nodes' trust evaluation to enhance the security and robustness. The practical applications of this method include the route, data integration and cluster head vote [1].

Although some existing approaches play good roles in improving security of other networks, trust management in WSNs still remains a challenging field. In this paper, we propose NBBTE algorithm by analyzing the advantages and disadvantages of existed methods [2-24]. Firstly, each node establishes the direct and indirect trust values of neighbor nodes by comprehensively considering various trust factors, and combining these factors together with network security grade, correlation of context time and rewards degree. The trust factors mentioned above include packet receive, send, strictness, delivery, consistency and availability, *etc*. Secondly, fuzzy set theory is used to decide the trustworthiness levels in accordance with the fuzzy subset grade of membership functions. Based on the levels of trustworthiness, the basic confidence function of D-S evidence theory is accordingly formed. Finally, using the revised Dempster rules of combination, the integrated trust value of a node is obtained by integrating its trustworthiness of multiple neighbor nodes.

The remainder of this paper is organized as follows. Section 2 introduces the related work. Section 3 describes the related notions and parameters. In Section 4, the proposed scheme is specifically depicted, including its design idea and practical implement approach. The performance of the scheme is mainly evaluated in Section 5. Finally, in Section 6, we make some concluding remarks.

2. Related Work

The trust management methods can be classified into two categories: distributive authorization system based on trust chain and network trust evaluation system based on nodes' behaviors [2-5]. (1) In the former system, the authorized individual is allowed to collect all the information of other authorized ones. It checks the consistency through strategy inference engine in light of local policy and authorization requirements. In addition, if a trust chain exists between two strange individuals, the authorization is able to be relayed by signing indirect objects which have trust rights. That is to say, the authorization individual has rights to deal with its trusted objects. But it is very dangerous for the limited resources of WSNs when the authorization nodes are compromised. (2) In the latter system, individuals acquire all kinds of related information, including the actions of evaluated individuals, interacting rules and other individuals' opinions. Then, the sensor nodes obtain other nodes' trust value by different computing method in application. This trust management method has advantages of less resources consumption, peer-to-peer structure and no centers. Therefore, trust management schemes similar to the latter one are more frequently applied in the WSNs.

Viljanen [6] came up with all kinds of ingredients of trust evaluation after nearly ten years of research on the trust of the network, which has a guiding effect on trust measurement of the sensor nodes in WSNs. Crosby *et al*. [7] propose a trust evaluation model based on the classical probability model, which uses simple statistical methods to accomplish trust value computation without considering the trust recommendation between sensor nodes. Therefore, it cannot reflect nodes' real-time trust state accurately. Ganeriwal *et al*. [8] make a trust evaluation model and uncertainty analysis based on Bayes theory. Because the lack of prior knowledge about wireless sensor networks, the model's subjective assumptions of prior distribution aggravates the uncertainty of trust. These two models both regard the subject fuzziness of trust as the randomness and use pure probability statistic method to assess trustworthiness, which is difficult to obtain prior knowledge from practical application and inevitably result in something unreasonable.

In order to deal with the subjective fuzziness of trust evaluation, Tang *et al*. [9] propose a trust evaluation model based on fuzzy logic, which provides a formalized inference mechanism and does not give specific trust calculation methods. Krasniewski *et al*. [10] use the base station to make a centralized trust management of cluster head election. If the cluster head is unbelievable, a new one will be elected in another round to avoid effectively malicious or selfish node to act as cluster head. But the centralized trust management model increases the network communication payload and the passive trust decision-making slows down the convergent speed of cluster head election. Song *et al*. [11] add trust component to the LEACH algorithm, where nodes select the highest trust value one from their neighbors as cluster head. Although the distributed algorithm in this scheme has high convergent speed, reputation-based trust management may be vulnerable to collusion attacking. TRANS [12,13], which is proposed by Tanachaiwiwat *et al*., searches and marks the suspicious positions in WSNs based on the geographic information route. It puts the nodes at the suspicious positions on a black list and broadcasts them to all the other nodes, thereby achieving trust-based secure routing. But there is the possibility that some nodes are misjudged to be malicious because of the abominable channel or compromised nodes. Consequently, it requires a mechanism to allow the nodes in black list to turn into usable nodes again, whereas the model neglects this point. Hur *et al*. [14,15] divide the network into

several grids, which accomplishes secure data integration by crosschecking the consistency of nodes' data, but collusion attacks are not able to be resisted very well.

PTM [16-18], a research sub-item of UBISEC (secure pervasive computing) supported by Europe IST FP6, which builds models mainly in accordance with revised D-S evidence theory, defines the inter-domain dynamic trust management based on the pervasive environment. The approach makes a strict punishment to malicious actions and has good computing convergence and scalability. But the shortage of the PTM is that it obtains indirect trust value on average without taking the fuzziness, subjectivity and uncertainty into account.

Hsieh *et al.* [19] use cluster-based structure to ensure the security of wireless sensor networks which includes two modules: (1) the dynamic key authorization is adopted to prevent external malicious nodes from entering when a new cluster is established or a new node joins in the cluster. (2) The nodes in the cluster detect each other and different trust computing methods are formulated based on the different roles nodes act as. The approach is difficult to implement and exists weak computing convergence.

Marmol *et al*. [20] carry out a wide review of different trust models, provide some pre-standardization recommendations and propose an interface proposal for trust models. Lopez *et al*. [21] list the best practices that are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices. These two references make an excellent summary, propose many profound viewpoints and show an additional insight on the trust evaluation field. In addition, other protocols [22-24] address trust management methods in self-organization networks from different views.

3. Preliminaries

In this section, we describe the overall architecture of the NBBTE and various parameter definitions, including all sorts of trust factors, the fuzzy subset grade of membership functions, the calculation methods of trust worthiness based on the D-S theory.

3.1. Definitions of Trust Factors

The trust relationship, developing from sociology and economics, has strong subjectivity and uncertainty. The accurate and applicable trust metric is the precondition of establishing nodes' trust degree. Some trust factors are analyzed from different viewpoints [15,16,20]. Inspired by these works, we define the composing elements of trust value according to the sensor nodes' behavioral features to resolve common attacks and protect the network [1,21]. When node *i* evaluates the trust degree on the node *j*:

(1) The factor of received packets rate $RPF_{i,j}(t)$: the change of node *j*'s received packets rate in period *t*.

(2) The factor of successfully sending packets rate $SPF_{i,j}(t)$: node *j*'s successful rate of sending packets in period *t*.

(3) The factor of packets forwarding rate $TPF_{i,j}(t)$: the relation between sent packets and received packets of node *j* in period *t.*

(4) The factor of data consistency $CPF_{i,j}(t)$: the degree of difference for sending data packets between node *j* and its neighbor nodes.

(5) The factor of time frequency $TFF(t)$: time relativity of context content in period *t.*

(6) The factor of node availability $HPF_{i,j}(t)$: the relativity between hello packets sent and ACK feedbacks received by node *i.*

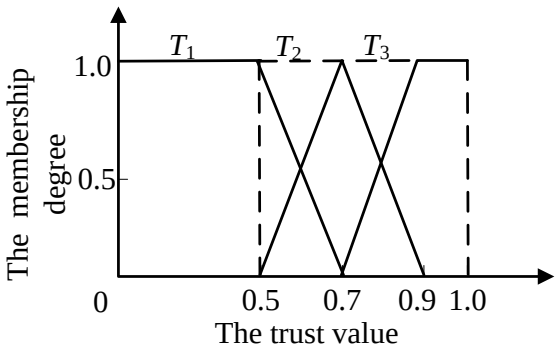
(7) Security grade SG: we define different security requirement according to the application fields of network (Battle field, emergency response, civil environment *etc*.).

3.2. Fuzzy Classification of Trust Relationship between Nodes

The trust degrees among sensor nodes are subjective and uncertain, which is decided by two aspects: (1) the classification of trust is not based on the 'two-valued logic' but 'multiple-valued logic'. (2) A certain trust value may belong to various trust grades rather than merely one grade. Thus, fuzzy theory is more suitable to describe and deal with fuzzy notions compared with traditional mathematical models. In this paper, we provide an efficient approach to make a quantitative research on subjective trust relationship by making the use of membership degree and language variables in the fuzzy theory.

The specific fuzzy classification of nodes' trust is as following. Firstly, the trust is divided into three grades: completely distrust, uncertain and completely trust state. Secondly, according to the three grades, it marks up three fuzzy subsets T_1, T_2 and T_3 on the universe of nodes' trust value T ([0,1]), as shown in Figure 1. The corresponding membership functions are $u_1(t)$, $u_2(t)$ and $u_3(t)$, $u_1(t) + u_2(t) + u_3(t) = 1$.

Figure 1. The membership function of node's trust.



3.3. Related Definitions and Rules in D-S Evidence Theory

The integrated trust value of one node given by its neighbor nodes cannot be simply established by weighted average due to the subjectivity of trust evaluation. While evidence theory proposed by Dempster and Shafer can briefly express the important conceptions, such as 'uncertainty' or 'not-knowing'. In addition, it makes right judgments by efficiently integrating many-sided uncertain information. Motivated by this, we take advantage of D-S evidence theory to compute integrated trust evaluation of nodes.

D-S evidence theory [25] is based on the Ω set comprised by basic propositions which are both exclusive and exhaustive, termed identification frame. 2^{Ω} is the power set of Ω, that is, the set of all the possible propositions based on Ω. Here we define Ω as $\{\boldsymbol{T}, -\boldsymbol{T}\}$, where $\boldsymbol{T}$ and $-\boldsymbol{T}$ represent two trust

states, namely credible and incredible. 2^{Ω} is $\{\Phi,\{\boldsymbol{T}\},\{-\boldsymbol{T}\},\{\boldsymbol{T},-\boldsymbol{T}\}\}$, in which Φ, $\{\boldsymbol{T}\}$, $\{-\boldsymbol{T}\}$ and $\{\boldsymbol{T},-\boldsymbol{T}\}$ represent respectively the empty set, the propositions of nodes' 'Trust', 'Distrust' and 'Uncertain'. There are definitions of basic reliability function m on 2^{Ω}:$2^{\Omega} \rightarrow [0,1]$, reliability function Bel: $2^{\Omega} \rightarrow [0,1]$ and likelihood function Pl: $2^{\Omega} \rightarrow [0,1]$, satisfying the following equations:

$$\begin{cases} m(\varnothing) = 0 \\ \sum_{A \subseteq \Omega} m(A) = 1, A \neq \varnothing \end{cases} \tag{1}$$

$$Bel(A) = \sum_{B \subseteq A} m(B), \forall A \subseteq \Omega \tag{2}$$

$$Pl(A) = 1 - Bel(\overline{A}), \ \forall \ A \subseteq \Omega \tag{3}$$

where: A is named focal element, $m(A)$ is the basic confidence level of A, representing how much the evidence support A to happen. $Pl(A)$ and $Bel(A)$ are the confidence level and likelihood of A, $Bel(\boldsymbol{T}) = m(\{\boldsymbol{T}\})$, $Pl(\boldsymbol{T}) = m(\{\boldsymbol{T}\}) + m(\{\boldsymbol{T}, -\boldsymbol{T}\})$.

In our proposed algorithm, the nodes evaluate each other to acquire some of the seven trust degrees which are the probability forms. To reflect the subjectivity, uncertainty and fuzziness of trust, we transform probability forms of the trust degrees to the vector forms by using fuzzy membership function and D-S evidence theory, and each element in this vector represents the calculated basic confidence level to the 'Distrust', 'Uncertain', 'Trust' propositions of nodes.

As for the integrated trust value which should combine the direct and indirect trust values, we make a combination of multiple evidences according to the revised Dempster rule, which will be described in detail in Section 4.2.2.

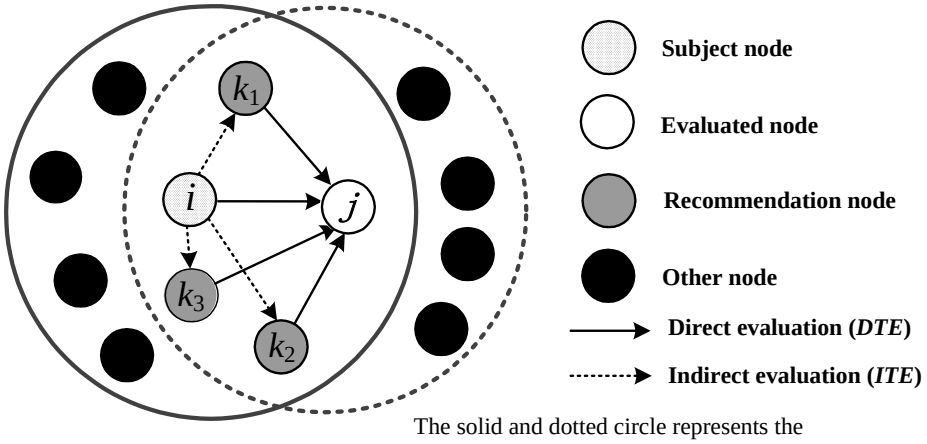
4. NBBTE Algorithm

As described in the introduction, the NBBTE algorithm firstly establishes various trust factors depending on the interactions between neighbor nodes, which are observed by each other. Then the trust value is obtained by combining network security degree and correlation of time context. Secondly, it applies the fuzzy set theory to measure how much the trust value of node belongs to each trust degree. Finally, the integrated trust value of evaluation considering the recommendation of several neighbor nodes is acquired in accordance with the trust difference between evidences and the revised Dempster rule of combination.

4.1. Trust Evaluation Approach between Neighbor Nodes

Trust depends on a subject's (evaluating node) observation on the object (evaluated node) and third party recommendations. The WSNs' features need a trust evaluation mechanism without central nodes, where neighbor nodes monitor each other. The subject obtains the trust value of objects according to both direct and indirect trust values. As shown in Figure 2, the node i is subject, which not only makes direct assessment of object j, but also makes indirect evaluation of object j through nodes k_1, k_2, k_3.

Figure 2. The recommendation trust relationship among nodes.



The solid and dotted circle represents the communication range of node *i* and *j*, respectively.

4.1.1. Trust Factors

It is essential to make quantitative and qualitative analysis of various factors which affect trust value in order to evaluate a node's trust worthiness. In the following, we explain the establishment scheme of trust factors defined in Section 3.1. We assume that node *i* makes trust evaluation for node *j* and ACK mechanism is adopted. In other words, once the node receives a packet, it sends ACK feedback information to the sender.

(1) The factor of received packets rate $RPF_{i,j}(t)$: According to the assumption, if node *i* monitors node *j* to confirm how many common ACK packets node *j* sends, the ratio of packets received by node *j* can be obtained. According to the change of the ratio, we can know whether node *j* has response forging behavior. If the change maintains in the interval $(-\xi, \xi)$ in different periods, node *j* works normally. The calculation equation is as follows ($RP_{ij}(t)$ represents the number of received packets):

$$RPF_{i,j}(t) = \frac{RP_{ij}(t) - RP_{ij}(t-1)}{RP_{ij}(t) + RP_{ij}(t-1)} \tag{4}$$

(2) The factor of successfully sending packets rate $SPF_{i,j}(t)$: Assume that *j* sends packets to *k* who is beyond the communication scope of *i*. Although *i* cannot monitor the successfully sent packets rate of *j* directly in this situation, node *i* can monitor the number of the same packets sent by *j*. It's known that every packet sent by nodes contains a time stamp and can be distinguished efficiently even if the packets have the same content. Thus, we can obtain the sending number of a certain packet according to different time stamps. The equation as follows ($SP_{ij}(t)$ is the needing number of sent packets, $SF_{ij}(t)$ is the repeating number of sent packets):

$$SPF_{i,j}(t) = \frac{SP_{ij}(t)}{SP_{ij}(t) + SF_{ij}(t)} \tag{5}$$

(3) The rate of data forwarding $TPF_{i,j}(t)$: Multi-hop is usually necessary since most of nodes are impossible to communicate with the base station directly. If node *k* is beyond the communication range of node *i* and sends data packets to node *j*, node *i* cannot monitor the received packets number of node

j directly and has to collect the ACK feedback information of node *j* to obtain the number of received packets. In order to distinguish the forwarding packets and the remained packets, an ACK packet which contains a special bit is constructed. Once node *j* receives a forwarding packet, it broadcasts an ACK packet above. Then node *i* can collect these ACK packets of node *j* to obtain the number of forwarding packets. According to the change rate of $TPF_{i,j}(t)$, it can efficiently avoid Sinkhole attack and Sybil attack, as well as identify whether the node is selfish. The equation as follows ($FP_{ij}(t)$ is the number of transmission packets):

$$TPF_{i,j}(t) = \frac{FP_{ij}(t) - FP_{ij}(t-1)}{FP_{ij}(t) + FP_{ij}(t-1)} \tag{6}$$

(4) The consistency factor $CPF_{i,j}(t)$: The data packets have spatial correlation, that is, the packets sent among neighbor nodes are similar in the same area according to the application. So the consistency factor is introduced to prevent malicious nodes from modifying primary data packets. Node *i* acquires a packet transmitted by *j* randomly and makes the comparison with its own data. If the source node of this packet is in the same area of node *i* and the diversity rate maintains in the interval $(-\xi, \xi)$, the number of accordant packets increases. Elsewise, if the source node does not belong to the area of node *i*, the consistency factor between node *i* and node *j* would not be adopted. The $CPF_{i,j}(t)$ equation as follows ($EP_{ij}(t)$ is the number of accordant packets, $NEP_{ij}(t)$ is the discordant one):

$$CPF_{i,j}(t) = \frac{EP_{ij}(t)}{EP_{ij}(t) + NEP_{ij}(t)} \tag{7}$$

(5) Time factor $TFF(t)$: Trust value has context relationship in time and content, and changes on the previous base. The size of time grade is dependent on the specific situation. If it is established too large, integrated trust value will be affected by history too heavily, which may cause errors in node evaluation. On the contrary, if it is established too small, trust value relies on a single period overly. Above all, we have the rules based on the security degree of networks. When the security degree is relatively high, $TFF(t) = 0.8$, relatively low, $TFF(t) = 0.2$, normally, $TFF(t) = 0.5$.

(6) The factor of availability $HPF_{i,j}(t)$: In some cases, the neighbor nodes are inaccessible due to wireless channel interference or bad environment. Concretely, node *i* sends HELLO packets for the detection whether they can be received by node *j*. If node *i* receive the ACK-HELLO packets from node *j*, it is proved that node *j* is accessible. The $HPF_{i,j}(t)$ equation as follows ($ACK_{ij}(t)$ is the amount of packets which have been responded, $NACK_{ij}(t)$ is the amount of packets which haven't been responded):

$$HPF_{i,j}(t) = \frac{ACK_{ij}(t)}{ACK_{ij}(t) + NACK_{ij}(t)} \tag{8}$$

(7) Security grade SG: According to specific application environment and scenario, the WSNs require different security degree based on different needs. For instance, there is a large difference between batter filed application and environmental monitor. When security requirement is high, SG = 3, relatively low, SG = 1; normally, SG = 2.

4.1.2. Trust Calculation between Neighbor Nodes

As shown in Figure 2, trust evaluation of the subject to object includes direct evaluation *DTE* and indirect evaluation *ITE*. For example, if node *j* is evaluated, node *i* not only obtains the trust value of node *j* by itself directly but also through k_1, k_2 and k_3 indirectly. And then node *i* integrates the two kinds of trust values to get an integrated one (for node *j*). Trust in the network has the feature 'hard to acquire and easy to lose'. There are two trust initialization strategies: the pessimistic and the optimistic strategy. The pessimistic strategy can eliminate the possibility that the malicious node creates a new identity and impersonates a new node to rejoin in the network with the purpose of throwing away its bad trust value [21]. While the optimistic one has the foundation of completely trust at the beginning of network deployment, and is propitious to the quick network expansion. Therefore, in the initial period, trust value between neighbor nodes is depended on the factual application. Then, the trust of nodes changes gradually depending on behavior, history and time.

(1) *DTE* Evaluation Approach

For ensuring the reasonability of trust evaluation approach, different action parameters μ must be constituted in the different periods. For instance, in one period, node *i* and *j* interact with each other 10,000 times and the satisfactory actions are 5,000. In another period, they interact 1,000 times and the satisfactory actions are 500. Both periods have a satisfactory action rate of 0.5, obviously, the former is more believable. Therefore, we have the action parameter equation as follows:

$$\mu = \frac{S_{ij}(t) / (F_{ij}(t) + S_{ij}(t))}{S_{ij}(t-1) / [F_{ij}(t-1) + S_{ij}(t-1)]} \tag{9}$$

where: $S_{ij}(t)$ is the number of success, $F_{ij}(t)$ is the number of failure. In accordance with the trust factors in Section 4.1.1, combining with node recourse and network function environment, the direct trust value $DTE_{i,j}(t)$ is:

$$\begin{aligned} DTE_{i,j}(t) = \mu^{SG} \times TFF(t) \times [w_1 \times (1 - |RPF_{i,j}(t)|) + w_2 \times |SPF_{i,j}(t)| + w_3 \times (1 - |TPF_{i,j}(t)|) \\ + w_4 \times |CPF_{i,j}(t)| + w_5 \times |HPF_{i,j}(t)|] + (1 - TFF(t)) \times DTE_{i,j}(t-1) \end{aligned} \tag{10}$$

where: w_1, w_2, w_3, w_4, w_5 are trust factor weights. They are independent with each other and adjustable with different practical applications and satisfy:

$$w_1 + w_2 + w_3 + w_4 + w_5 = 1 \tag{11}$$

(2) *ITE* Evaluation Approach

Evaluation subject *i* collects other nodes' opinions on the evaluated object *j* as the indirect recommendation values. In order to decrease network communication payload and avoid trust recycle recursion, the recommendation values are confined to direct trust value of the common neighbors owned by both node *i* and *j*. As shown in the Figure 2, node *i* can only get the trust recommendation of *j* from k_1, k_2 and k_3. Trust recommendation value is as follows according to the principle of trust transfer decline:

$$ITE_{i,j}(t) = DTE_{i,k}(t) \times DTE_{k,j}(t) \tag{12}$$

where *k* is the common neighbor of both node *i* and *j*.

4.2. The Method of Integrated Trust Value

Generally, the evaluated object has many neighbor nodes, and every neighbor has the direct trust value and indirect trust value of the evaluated object. To realize the fuzziness, subjectivity and uncertainty of trust evaluation, the D-S evidence theory method is adopted to obtain the integrated trust value instead of the simple weighted-average one.

The trust value of evaluation made by subject to object is obtained in Section 4.1. Based on it, we use the membership function of nodes' trust classification to calculate the basic confidence level of trust evidence to the 'Distrust', 'Uncertain', 'Trust' propositions of nodes. Then the integrated trust value of the object is acquired by composing the direct and indirect trust value which is based on the revised Dempster integration rules.

4.2.1. Trust Vector

In the process of integrating trust, the trust level of node *i* to *j* is indicated in vector form. The direct, indirect and integrated trust vectors of node *i* to *j* are:

$$\begin{aligned} &VDTE_{i,j}(t) = (m_{i,j}^{D}(\{-T\}), m_{i,j}^{D}(\{T,-T\}), m_{i,j}^{D}(\{T\})) \\ &VITE_{i,j}^{k_1}(t) = (m_{i,j}^{k_1}(\{-T\}), m_{i,j}^{k_1}(\{T,-T\}), m_{i,j}^{k_1}(\{T\})) \\ &\ldots \\ &VITE_{i,j}^{k_l}(t) = (m_{i,j}^{k_l}(\{-T\}), m_{i,j}^{k_l}(\{T,-T\}), m_{i,j}^{k_l}(\{T\})) \\ &VAT_{i,j}(t) = (m_{i,j}(\{-T\}), m_{i,j}(\{T,-T\}), m_{i,j}(\{T\})) \end{aligned} \tag{13}$$

According to Equations (10) and (12), the probability forms of direct and indirect trust value of object *j* what the subject *i* gets are defined as $DTE_{i,j}(t)$ and $ITE_{i,j}(t)$. Using the corresponding membership functions in Section 3.2, we compute the fuzzy membership grades of node *j* to the 'Distrust', 'Uncertain' and 'Trust' grade. The fuzzy membership grades of $DTE_{i,j}(t)$, u_1^{D}, u_2^{D}, u_3^{D}, and the grades of $ITE_{i,j}(t)$, u_1^{I}, u_2^{I}, u_3^{I} are calculated by:

$$\begin{cases} u_1^D = u_1(DTE_{i,j}(t)) \\ u_2^D = u_2(DTE_{i,j}(t)) \\ u_3^D = u_3(DTE_{i,j}(t)) \end{cases} \text{ and } \begin{cases} u_1^I = u_1(ITE_{i,j}(t)) \\ u_2^I = u_2(ITE_{i,j}(t)) \\ u_3^I = u_3(ITE_{i,j}(t)) \end{cases} \tag{14}$$

If we regard the membership function of nodes' trust classification as the basic confidence function of propositions$\{-\boldsymbol{T}\}\{\boldsymbol{T}, -\boldsymbol{T}\}\{\boldsymbol{T}\}$, $u_1(t)$, $u_2(t)$ and $u_3(t)$ respectively stand for the support levels of trust evidences to the 'Distrust', 'Uncertain' and 'Trust' grade. At this point, $m_{i,j}^{D}(\{-\boldsymbol{T}\})$, $m_{i,j}^{D}(\{\boldsymbol{T}, -\boldsymbol{T}\})$ and $m_{i,j}^{D}(\{\boldsymbol{T}\})$, the components of direct trust vector $VDTE_{i,j}(t)$, are respectively equal to u_1^{D}, u_2^{D} and u_3^{D}. Similarly, $m_{i,j}^{k}(\{-\boldsymbol{T}\})$, $m_{i,j}^{k}(\{\boldsymbol{T}, -\boldsymbol{T}\})$ and $m_{i,j}^{k}(\{\boldsymbol{T}\})$, the components of indirect trust vector $VITE_{i,j}(t)$, correspond to u_1^{I}, u_2^{I} and u_3^{I}, respectively.

4.2.2. Integrating the Trust Value

In this section, we combine the direct and indirect trust values of node *j* to get the integrated trust value. The integration process is in accordance with the revised Dempster combination rule, which is described in detail in the following.

Assume that Bel_1 and Bel_2 are two trust degree functions that on the same recognizing frame Ω, their basic trust degree function are m_1 and m_2. If $\sum_{X \cap Y=\emptyset} m_1(X) \times m_2(Y) < 1$, the orthogonal of Bel_1 and Bel_2 is $Bel = Bel_1 \theta Bel_2$, where $A \in \Omega$. And m, the basic trust degree function of Bel can be expressed as follows:

$$\begin{cases} m(A) = m_1(A) \oplus m_2(A) = \dfrac{\sum\limits_{X \cap Y=A} m_1(X) \times m_2(Y)}{1-K} \\ A \neq \emptyset, \ A \subseteq \Omega \\ m(\emptyset) = 0 \end{cases} \tag{15}$$

$$K = \sum_{X \cap Y=\emptyset} m_1(X) \times m_2(Y) \tag{16}$$

As shown in Figure 2, at the end of period t, node i makes an integrated trust evaluation on node j. From human's action model and the trust's subjectivity, we know that the weight of direct and indirect trust values shouldn't be the same. The weight of $VDTE_j(t)$ and $VITE_j(t)$ should be modified. Assume the weight of direct trust value is 1, and the indirect evidence's weight is changed according to the similarity between direct and indirect trust value. On this basis, we use the Equations (15) and (16) to calculate the integrated trust value $VAT_{i,j}(t)$ (subject i to object j).

Next, the course of modification evidential weight is described. If node i gets l indirect trust values to evaluated node j, the difference between any indirect and direct evidence are as follows:

$$D_{k_n,i}(t) = \sqrt{\frac{1}{2}(\overrightarrow{m_{i,j}^{k_n}} - \overrightarrow{m_{i,j}^{D}})^T D(\overrightarrow{m_{i,j}^{k_n}} - \overrightarrow{m_{i,j}^{D}})} = \sqrt{\frac{1}{2}(\left\|m_{i,j}^{k_n}\right\|^2 + \left\|m_{i,j}^{D}\right\|^2 - 2\left\langle \overrightarrow{m_{i,j}^{k_n}}, \overrightarrow{m_{i,j}^{D}} \right\rangle)} \tag{17}$$

The $\overrightarrow{m_{i,j}^{kn}}$ and $\overrightarrow{m_{i,j}^{D}}$, defined in the Equation (13), are indirect and direct trust vector, respectively. When the evidence difference $D_{kn,i} > \xi$, it usually means that a malicious node is sending bogus information. Then, the similarity parameter between different evidences is modulated according to Equations (13) and (17):

$$S_{k_n,i}(t) = 1 - D_{k_n,i}(t) \tag{18}$$

From the Equation (18), the modified weight of indirect evidence is:

$$\begin{cases} \Delta m_{i,j}^{k_n}(\{T\}) = S_{k_n,i}(t) * m_{i,j}^{k_n}(\{T\}) \\ \Delta m_{i,j}^{k_n}(\{-T\}) = S_{k_n,i}(t) * m_{i,j}^{k_n}(\{-T\}) \\ \Delta m_{i,j}^{k_n}(\{T,-T\}) = 1 - m_{i,j}^{k_n}(\{T\}) - m_{i,j}^{k_n}(\{-T\}) \end{cases} \tag{19}$$

Above all, the indirect evidence can be modified as:

$$\Delta VITE_{i,j}^{k_n}(t) = (\Delta m_{i,j}^{k_n}(\{-T\}), \Delta m_{i,j}^{k_n}(\{T,-T\}), \Delta m_{i,j}^{k_n}(\{T\})) \tag{20}$$

According to Equations (10), (15), (16) and (20), the integrated trust value is as follows:

$$m_{i,j}(A) = m_{i,j}^{D}(A) \oplus \frac{1}{l}\sum_{n=1}^{l} \Delta m_{i,j}^{k_n}(A) \tag{21}$$

Finally [26], the eventual basic confidence assignment value is established by Equation (21), if the decision model satisfies:

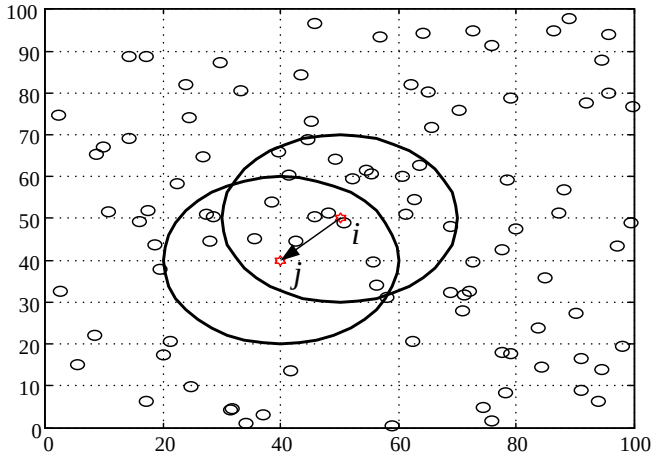
$$\begin{cases} m_{i,j}(\{T\}) - m_{i,j}(\{-T\}) > \varepsilon \\ m_{i,j}(\{T,-T\}) < \theta \\ m_{i,j}(\{T\}) > m_{i,j}(\{T,-T\}) \end{cases} \quad (22)$$

Then main subject node *i* regards node *j* as trust, and add node *j* into its trustworthiness list. In like manner, node *j* can be marked 'Uncertain' or 'Distrust'.

5. Simulations

We used MatLab as simulation tool to analyze the performances of the NBBTE algorithm in this section, which includes: trust evaluation of credible nodes, incredible nodes, and malicious nodes, as well as the influence of factors on the trust evaluation. The concrete simulation scene is a square area of 100 m × 100 m, with 100 randomly deployed nodes. Here the communication radius is 20 m. We assume node *i* is subject node and node *j* is evaluated node, overlapping part of two circles is the common neighbor of evaluation and evaluated node (Figure 3). From the viewpoint of rigorous security requirement, the pessimistic initialization strategy of trust value is adopted, and the initial trust state of nodes is set as incredible. Some parameters vary with the scenes and the purposes of experiment and will be explained in detail.

Figure 3. The distribution map of random nodes.



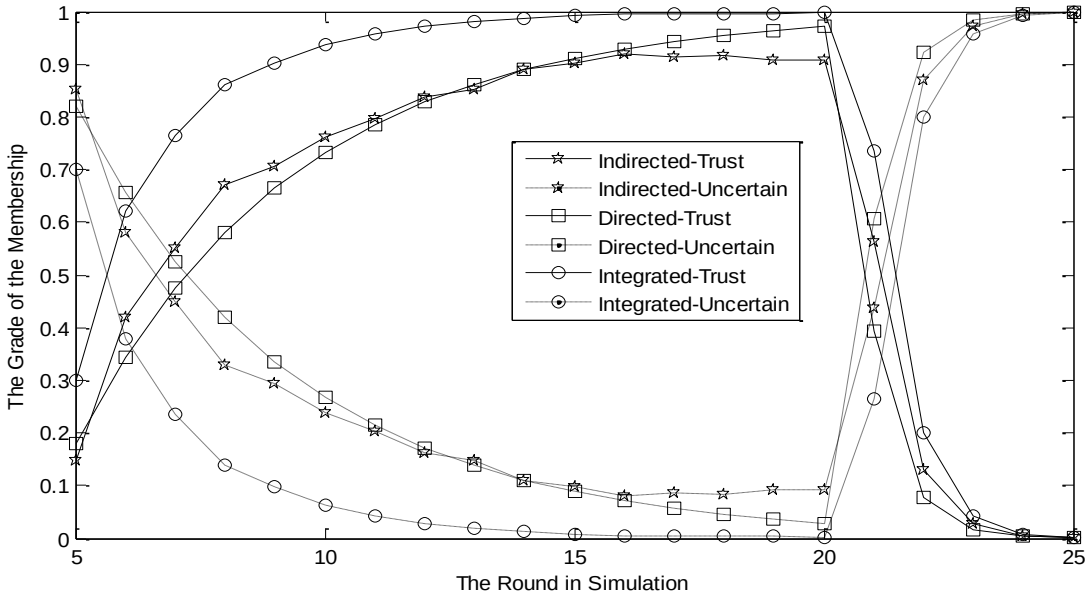
i - subject node, j - evaluated node

5.1. Analysis of Trust Evaluation

Preferences: In this section, $w_1 = w_2 = w_3 = w_4 = w_5 = 0.2$, security degree SG = 1, behavioral coefficient $\mu = 1$, time factor $TFF(t)$ changes with nodes' trust value. When the trust value of node *j* increases gradually, $TFF(t) = 0.2$, in contrast, $TFF(t) = 0.8$. If all the change rates of trust factors are in the range of 10% ~ 20%, node *j* is thought to be a non-malicious node, else if the change rates are 50%, node *j* is abnormal and has malicious or self actions.

The change tendency of node membership grade to three basic trust degree functions reflects the effectiveness of revised D-S evidence theory. In this section, the character of 'trust is hard to acquire and easy to lose' should be expressed. Simulation results are shown in Figure 4.

Figure 4. The membership grade of the distrustful actions.



Firstly, we assume the actions of each node in network are normal. In Figure 4, when the trust evaluation system tends to be stable, trust value of node *j* increases slowly. Therefore, its membership grade to 'Trust' increases gradually and the one to 'uncertain' accordingly decreases. Meanwhile, integrated trust value is higher than both direct and indirect trust value. That is because the proposed scheme adopts D-S theory to integrate trust values of nodes which lends the reality of node *j* to be represented better. On the contrary, using the weighted-average method, integrated trust value is lower than direct trust value, which fails to show the advantage of trust value integration.

Secondly, in order to reflect that the NBBTE can achieve the character of 'trust is hard to acquire and easy to lose', we assume the actions of each node in network are abnormal when the trust value measure up to the peak. It can be seen from Figure 4 that the evaluation model reflects nodes' change in acutely behavior and has more sensitive change to malicious actions. The trust value increases slowly for fifteen periods when a node collaborates well with others. However, when the node begins to uncooperative, its trust value decreases quickly to nearly zero in only four periods. This result verifies the NBBTE represents the character 'trust is hard to acquire and easy to lose'.

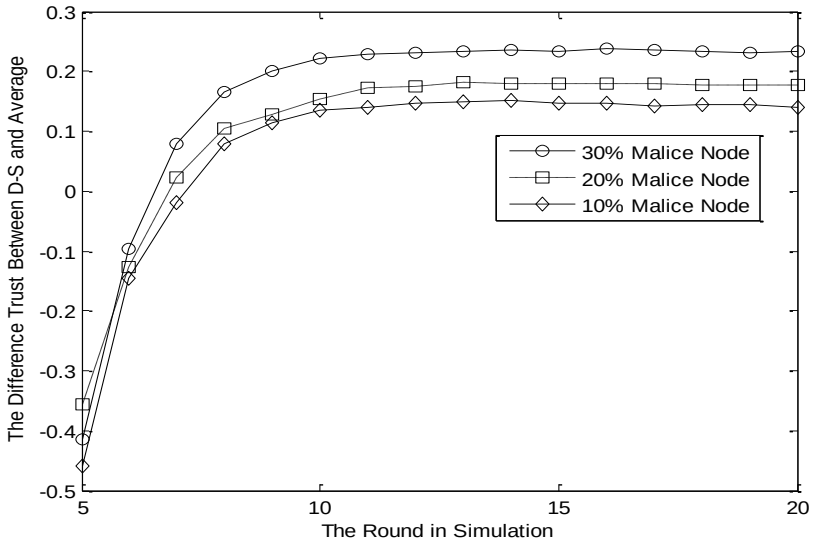
5.2. The Influence of Malicious Nodes

Preferences: the number of malicious nodes in the common neighbors of both node *i* and *j* are 10%, 20% and 30%, respectively. Other preferences are the same as Section 5.1. Most existing trust evaluation algorithms adopt the average methods to calculate the trust value of evaluated nodes, which can not reflect the actual contribution of different subject nodes (direct and indirect nodes).

In this section, the function of NBBTE algorithm is assessed by introducing different proportions of malicious nodes, which send bogus indirect trust values. The trust difference between average method and the proposed scheme is used to show the advantages of NBBTE algorithm. Assume that evaluation subject *i* is credible and the membership degrees of malicious nodes are opposite compared with normal ones. We can see from Figure 5 that the two schemes in membership degree to 'TRUST' tend to be stable gradually with evaluation time, but the more the malicious nodes, the greater the

difference. That's because that NBBTE algorithm applies the revised Dempster rule of combination, which modulates indirect weight according to the evidence differences between direct and indirect trust value. Thus, the proposed scheme takes fuzziness and subjectivity of trust in consideration. With the increasing of malicious nodes, weight modulation shows more advantage.

Figure 5. The comparison between NBBTE and weighed-average method.



6. Conclusions

In order to identify selfish and malicious nodes efficiently and solve the security problems for node failure or capture in WSNs, this paper proposes a trust evaluation algorithm based on behavior strategy banding D-S belief theory, which successfully underlines the fuzziness, subjectivity and usability of trust. The core works of the algorithm (NBBTE) include the following parts:

Establish trust factors by considering network's practical application environment. Then make both quantitative and qualitative analysis to calculate the direct and indirect trust value.

Obtain the membership degree of trust value to trust grade by fuzziness set theory and accordingly form the basic input vector of evidence theory.

Revise the Dempster rule of combination and modulate similarity coefficient in accordance with differences between indirect and direct evidences to integrate the trust value of evaluated node.

At the end, the simulations show that the scheme can assess nodes' trustworthiness efficiently accounting for subjectivity, uncertainty and fuzziness of trust evaluation. Furthermore, it can represent the feature that 'trust is hard to acquire and easy to lose' and improve the security of networks.

The process of trust evaluation may need excess energy and time costs due to the cooperation and communication with neighbors, and the memory costs also increase with the parameter numbers, algorithm precision and network density. However, to enhance the network security, a compromise has to be made between the trust and the resource consumption. And we believe that the resource constraint of nodes is likely to be resolved in the future due to the technical development.

As future work a real experiment is being designed to estimate the performance of algorithm. Moreover, applications based on node trust are being considered, such as routing, data aggregation and so on.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 60873240 and No. 60974121, the National High Technology Research and Development Program of China (863 Program) under Grant No. 2009AA01Z201 and Beijing Municipal Education Commission. The authors would also like to thank the paper's anonymous reviewers for their insightful comments.

References

1. Jing, Q.; Tang, L.Y.; Chen, Z. Trust Management in Wireless Sensor Networks. *J. Softw.* **2008**, *19*, 1716-1730.
2. Blaze, M.; Feigenbaum, J.; Lacy, J. Decentralized Trust Management. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2002; pp. 164-173.
3. Ellison, C.M.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B.M.; Ylonen, T. *Simple Public Key Infrastructure Certificate Theory*; Available online: http://www.ietf.org/ietf/1id-abstracts.txt (accessed on 9 December 2010).
4. Li, N.H.; Mitchell, J.C. RT: A Role-Based Trust-management Framework. In *Proceedings of the 3rd DARPA Information Survivability Conference and Exposition*, Washington, DC, USA, April 2003; pp. 201-212.
5. Li, N.H.; Mitchell, J.C.; Winsborough, W.H. Beyond Proof-of-Compliance: Security Analysis in Trust Management. *J. ACM* **2005**, *52*, 474-514.
6. Viljanen, L. Towards an Ontology of Trust. In *Proceedings of the TrustBus 2005, LNCS 3592*, Copenhagen, Denmark, 22–26 August 2005; pp. 175-184.
7. Crosby, G.V.; Pissinou, N.; Gadze, J. A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks. In *Proceedings of Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Columbia, MD, USA, April 2006; pp. 13-22.
8. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-Based Framework for High Integrity Sensor Networks. *ACM Trans. Sens. Netw*. **2008**, *4*, 1-37.
9. Tang, W.; Hu, J.B.; Chen, Z. Research on a Fuzzy Logic-Based Subjective Trust Management Model. *J. Comput. Res. Develop.* **2005**, *42*, 1654-1659.
10. Krasniewski, M.; Varadharajan, P.; Rabeler, B.; Bagchi, S.; Hu, Y.C. TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks. In *Proceedings of the 2005 International Conference on Dependable Systems and Networks*, Yokohama, Japan, June 2005; pp. 672-681.
11. Song, F.; Zhao, B.H. Trust-Based LEACH Protocol for Wireless Sensor Networks. In *Proceedings of the Second International Conference on Future Generation Communication and Networking*, Yokohama, Japan, 13–15 December 2008; pp. 202-207.
12. Tanachaiwiwat, S.; Dave, P.; Bhindwale, R.; Helmy, A. Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-aware Sensor Networks. In *Proceedings of the SenSys*, Los Angeles, CA, USA, November 2003; pp. 324-325.

13. Tanachaiwiwat, S.; Dave, P.; Bhindwale, R.; Helmy, A. Location-Centric Isolation of Misbehavior and Trust Routing in Energy-Constrained Sensor Networks. In *Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference*, Phoenix, AZ, USA, 15–17 April 2004; pp. 463-469.
14. Hur, J.; Lee, Y.; Hong, S.M.; Yoon, H. Trust Management for Resilient Wireless Sensor Networks. In *Proceedings of the 8th International Conference on Information Security an Cryptology*, Seoul, Korea, December 2005; pp. 56-68.
15. Hur, J.; Lee, Y.; Yoon, H.; Choi, D.; Jun, S.; Trust Evaluation Model for Wireless Sensor Networks. In *Proceedings of the 7th International Conference on Advanced Communication Technology*, Phoenix Park, Korea, 21–23 February 2005; pp. 491-496.
16. Almenarez, F.; Marin, A.; Diaz, D.; Sanchez, J. Developing a Model for Trust Management in Pervasive Devices. In *Proceedings of 4th IEEE Annual International Conference on Pervasive Computing and Communications*, Pisa, Italy, March 2006; pp. 267-271.
17. Almenarez, F.; Marin, A.; Campo, C.; Garcia, R.C. PTM: A Pervasive Trust Management Model for Dynamic Open Environments. In *Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust*, Boston, MA, USA, August 2004.
18. Almenarez, F.; Marin, A.; Campo, C.; Garcia, R.C. TrustAC: Trust-based Access Control for Pervasive Devices. In *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, Boppard, Germany, April 2005; pp. 225-238.
19. Hsieh, M.Y.; Huang, Y.M.; Chao, H.C. Adaptive Security Design with Malicious Node Detection in Cluster-Based Sensor Networks. *Comput. Commun.* **2007**, *30*, 2385-2400.
20. Marmol, F.G.; Perez, G.M. Towards Pre-standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems. *Comput. Stand. Interfaces* **2010**, *32*, 185-196.
21. Lopez, J.; Roman, R.; Agudo, I.; Fernandez, C.G. Trust Management Systems for Wireless Sensor Networks: Best Practices. *Comput. Commun.* **2010**, *33*, 1086-1093.
22. Li, J.L.; Gu, L.Z.; Yang, Y.X. A New Trust Management Model for P2P Networks. *J. Beijing Univ. Posts Telecommun*. **2009**, *32*, 71-74.
23. Li, J.L.; Gu, L.Z.; Yang, Y.X. A New Trust Management Model for P2P Networks with Time Self-Decay and Subjective Expect. *J. Electron. Inf. Technol.* **2009**, *31*, 2786-2790.
24. Li, L.; Fan, L.; Hui, H. Behavior-Driven Role-Based Trust Management. *J. Softw.* **2009**, *20*, 2298-2306.
25. Dempster, A. Upper and Lower Probabilities Induced by Multivalued Mapping. *Ann. Math. Stat.* **1967**, *38*, 325-339.
26. Chen, B.; Wan, J.W.; Wu, Y.F. A Pipeline Leakage Diagnosis for Fusing Neural Network and Evidence Theory. *J. Beijing Univ. Posts Telecommun*. **2009**, *32*, 5-9.