www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

Belief and Reputation Based Recommended Trust Computation in Wireless Sensor Networks

[1] Bo Zhang, [1*] Xiaosheng Pan, [2] Yang Xiang, [3] Tao Pan

[1] College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, P. R. China

[2] College of Electronics and Information Engineering, Tongji University, Shanghai, 201804, P. R. China

[3] Shen Hua Hollysys Information Technology, Co .Ltd. Beijing, 100000, P. R. China

[*] E-mail: itol_xs@shnu.edu.cn

Received: 16 May 2013 /Accepted: 12 August 2013 /Published: 20 August 2013

Abstract: Due to limited capacity of individual node, cooperation is a feasible solution to cope with complex task in wireless sensor networks (WSNs). However, node cooperation might be launched with an unreliable collaborative group in large-scaled WSN. To solve this challenge, a node can be organized through recommendation. In this paper, we propose a belief and reputation based recommended trust computation mechanism, which is used to build up creditable relationships among strange nodes. Firstly, we define subjective trustable relationship among nodes, named belief, and objective common trust view, named reputation, for nodes in WSNs. Then, we present a recommended trust computation based on aforementioned two notions. The recommended trust computation is divided into three aspects, i.e., recommended trust computation with different route composition, objective coincidence and optional degree. Furthermore, a recommended trust computation framework (RTCF) and its related proofs are proposed. Finally, we give example and examinations to further explain the efficiency and feasibility of our mechanism. *Copyright © 2013 IFSA.*

Keywords: Wireless sensor networks (WSN), Recommended trust, Belief, Reputation.

1. Introduction

Due to the ability of changing the world significantly, wireless sensor networks (WSNs) obtains more and more attentions in recent years [1-2]. Consisting of large number of tiny and cheap nodes, WSNs would meet the complicated application requirements through the cooperation of nodes. Different from the cooperation in wired network environments (e.g., Internet and Intranet), the cooperation in WSNs faces with some limitations because nodes are unreliable devices with features of weakness, temporary access, low power, and limited capacity. In such a network, node cooperation is vulnerable to threats and risks. Therefore the security of node selection is an unavoidable challenge of node cooperation. Once selecting an unreliable node, its weakness would definitely endanger the cooperation to achieve goals. In our consideration, the problem of securing node cooperation has been a roadblock to large scale application of WSNs. Research field of securing wireless sensor networks is still in its infancy.

In an open and dynamic environment, it is impossible for the node to recognize all the other thousands of nodes and to select appropriate nodes for cooperation, which means that nodes would be selected without any objective and creditable

Article number 1283

standards for measurement. Such embarrassing situation brings more unreliability to cooperation in WSNs. In recent years, trust has been suggested as an effective security mechanism for inspiring the cooperation organizing in network environment [2]. Through subjective or objective impressions, i.e., belief or reputation, one can make decisions for node selection depending on their trust evaluation. Some research work has shown that rating nodes' trust and reputation is an effective approach to improve security or promote node cooperation in WSNs [3, 6-10].

In this paper, we introduce a belief and reputation based recommended trust computation mechanism for node cooperation in WSNs. The rest of this paper is organized as follows. In Section 2, we propose the related works of this paper. In Section 3, we address the subjective trust relationship named belief between nodes and objective trust degree named reputation respectively. Then, we present the definition of recommended trust and the computation mechanism which is composed by three aspects: recommended trust computation with different route composition, recommendation objective coincidence and recommendation optional degree in section 4. And further, we address a recommended trust computation framework (RTCF) in this section. Moreover, we present some lemmas and theorems in order to prove the correctness for our mechanism in section 5. Finally, example was given to explain the efficiency and feasibility in section 6.

2. Related Works

The key problem, which lacks of enough attentions, is that traditional trust establishment mechanisms focus on providing trust relationship among nodes, ranking reputation for nodes or managing trust for nodes [11]. Such mechanisms are not efficient because there are a large number of sensor nodes and there are limited communications and unfamiliar relationships between nodes in WSNs. As aforementioned, it is impossible for a node to be familiar with all other ones so that it is indispensable for WSNs to help the node selecting strange ones in order to ensure the performance of cooperation based on most competent nodes. Moreover, wireless sensors networks are deployed in open, unsupervised and insecure environment which is prone to increase the risks of unsuccessful cooperation. And also the absence of any centralized authority in WSNs makes it challenging to monitor every node's reputation accurately. Hence, building cooperative relationships just depending on nodes' trust relationships or reputation is not a viable solution since evaluating trust relationship between every two nodes or scanning reputation would lead to large amounts of cost by flooding the network with request message [2].

Some existing researches aim to address recommended trust for WSNs, such as the ones given in [2, 4, 14, 16]. However, the recommended trust mechanisms in these researches are calculated based on subjective or objective views and ignored the comprehensive views. And also, some researches pay less attention to the recommendation route composition and only calculate recommended trust though single route or one intermediate recommender. In our consideration, recommendation is a feasible and effective solution. A Node can evaluate the trust degree of one who is recommended for cooperation. Recommendation builds up an initial trust relationships between strange nodes. Therefore, our motivation of this paper is to build up a mechanism of recommend trust evaluation for WSNs and make the recommendation fitting the truth of nodes.

3. Belief and Reputation

3.1. Belief Among Nodes

Trust, as an inherent willingness of human beings, shows the emotional and logic confidence relationships between peoples. It is derived from judging trustworthiness by evaluating various facts which can leads to the confidence or distrust. Firstly, we address the subjective trust notion which is named as belief in this paper. Belief demonstrates one's subjective willingness about others. As mentioned in reference [12], subjective trust is based on the ones the past experience and observation. We can define belief between nodes as following,

Definition 1. Belief is a node's subjective opinion towards another one based on the past interactions, judgments and result observations between nodes.

Let there be node d_i and d_j in WSNs, and d_j do n times of interaction with d_i in past. Each time of interaction generated a judgment value $jud_t(d_j)\left(jud_t(d_j)\in[0,1]\right)$ which was given by d_i for interaction with d_j. Assume that there were m times of malicious judgments from d_i to d_j. Let there be p nodes, $type(d_j)$, which are same type of node d_j and did direct interactions with d_i in past. $belief(d_i,type(d_j))$ indicates the belief from d_i to each same type nodes of d_j. Then, belief of past judgments can be calculated as following,

$$belief(d_i,d_j)=\begin{cases}\dfrac{\sum_{t=1}^{n}jud_t(d_j)}{n}\times\left(\dfrac{n-m}{n}\right)^{\frac{1}{n-m}} & n\neq 0\\ \alpha\times\dfrac{\sum belief(d_i,type(d_j))}{p} & n=0\end{cases}\qquad(1)$$

In formula 1, belief computation is based on the overall past judgments given by d_i. The number p

denotes the parameter $\alpha \in [0,1]$ reflects the impact to the initial belief from the type of target node. Contrast with traditional average computation of past judgments, we address an impact factor according to the result observations, i.e. total interaction quantity and malicious interaction quantity. In the impact factor calculation, malicious interaction would lead to belief reducing, which corresponds to the facts that people should execute more trustable actions to maintain their trust relationships while even a little of malicious actions would damage their trust relationships in human society.

3.2. Reputation

Reputation is a different complex notion from belief because reputation spans across multiple disciplines and is easily confused with trust [2]. Reputation denotes a public and authoritative trust view from an adiaphorous community [11].

In addition, due to the distributed nature of WSN, it is impossible to set a centralized reputation center to publish and renew each node's reputation. To reducing computation complexity and storage, distributed scheme is a feasible solution for reputation management. In this paper, we proposed a distributed reputation calculation method for nodes in WSN. Our method allows nodes to request local reputation records from creditable nodes and then combine the records with node's own reputation into a comprehensive value. Here, we proposed the reputation in WSN as follows,

Definition 2. Reputation is a global trustable view which combines the nodes' local reputation views in a working community.

Let there be a community D in WSNs, and $d_j \in D$. Assume that the set, CD, includes nodes which have reputation value larger than a threshold. For a node d_i in D, it received h times of judgment, $jud\left(d_j, d_i\right)$, in past. Hence, its reputation can be calculated as follows,

$$reputation(d_i) = \frac{\sum_{d_j \in CD} \left[jud\left(d_j, d_i\right) \times reputation(d_j) \right]}{h} \tag{2}$$

Similar to formula 1, reputation computation is not a simple average of past judgment. We appoint that only those nodes which have a good reputation can vote judgments to calculate reputation. Further, since the judgment given from various nodes in community, we add their own reputations as impact factor to enhance or weaken their judgments.

4. Recommended Trust

4.1. Single Route Recommended Trust

In large network environment, it is difficult to request for inquiring the reputation of every node, let alone obtain belief relationship between all nodes [4]. In WSNs, node can recognize strange ones through familiar nodes' recommendation. Through the recommendation, node of WSNs will evaluate the subjective belief impression from recommender, and also will measure the objective reputation of both the recommenders and the presentee. It is an integrated consideration for node. Recommended trust is built up through intermediate nodes that have beliefs with both recommendation demander and the recommended strange node. We divide recommendation into three cases according to different route compositions.

We first now present the simplest case of recommended trust computation method. Let the recommendation demander be $\Re$, the intermediate nodes as recommenders be $d_1, d_2, ...$, and the presentee strange node be $\Im$. Assume that the recommendation is a single-track and single route through $route = [\Re, d_1, d_2, ..., \Im]$ between $\Re$ and $\Im$.

Definition 3. Single route recommended trust is an integrated and single-track trust which consists of subjective beliefs of recommenders by transmitting methodology.

Single route recommended trust can be calculated as follows,

$$\begin{aligned} & sr(\Re, \Im) = \\ & \frac{1}{dep(\Im)} \times \{[belief(d_i, \Im) \times reputation(\Im)] \\ & + \sum_{i=1}^{dep(\Im)-1} \left[belief(d_{i-1}, d_i) \times reputation(d_i)\right] \\ & + \left[belief(\Re, d_1) \times reputation(d_1)\right]\} \end{aligned}, \tag{3}$$

where function $dep(\Im)$ indicates the route depth from $\Re$ to $\Im$ and $dep(\Im) = |route| - 1$.

In traditional researches, recommended trust is usually treated as a static transmitting value [4, 13, 14]. Nevertheless, recommendation is a sensitive and dynamic process. It builds up on subjective relationships between ones. In fact, recommended trust usually damps with the quantity of intermediate recommender rising. For example, it is possible to bring mistakes in recommendation if there were numerous intermediate links in a single-track recommendation in human society, what is called passing mouth to mouth leading to gossip. Likewise, in WSNs, recommended trust computation definitely should pay attention to such problem. In order to identify such evolution, we propose the damping effect of recommended trust. We modify above formula as following,

$$sr(\Re,\Im) = \frac{1}{dep(\Im)} \times \{[belief(d_i,\Im)\times reputation(\Im)]^{dep(\Im)} + \sum_{i=1}^{dep(\Im)-1}[belief(d_{i-1},d_i)\times reputation(d_i)]^{dep(\Im)-i+1} + [belief(\Re,d_1)\times reputation(d_1)]\} \tag{4}$$

The difference between formula 3 and 4 is that we add the route depth as impact exponent. The net result is that each node's recommendation would be weakened according to its depth in recommending route. That means distant recommendations are deemed less untrustworthy.

4.2. Multiple Routes Recommended Trust

In WSNs, demander node usually has various candidate nodes who can recommend the competent node for its recommendation request. In such case, the presentee node would be recommended to demander node through multiple routes. Therefore, recommended trust integrates with presentee node' reputation and the subjective believes of intermediate nodes.

As aforementioned, single route recommended trust can be calculated through the single-track belief transmitting among intermediate nodes, we now need to find out an effective and feasible mechanism which has capacity of combining multiple single route recommended trusts.

Different from single route recommended trust calculation, multiple routes recommended trust have two kinds of route composition in recommendation, i.e., independent routes and overlapping routes. Fig. 1 shows two kinds of route composition for multiple routes recommended trust.

Definition 4. Multiple routes recommended trust is an integrated trust which combines with single route recommended trusts in independent or overlapping routes from presentee node to demander node.

We first address the multiple routes recommended trust computation with independent routes. Let there be $m(m \geq 2)$ independent routes of recommendation between $\Im$ and $\Re$, each independent route can be identified as $route_k$, and each independent single route recommended trust be $sr_k(\Im)$. Then, multiple routes recommended trust can be calculated as follows,

$$mr(\Re,\Im)\_ = \min\left[\frac{\sum_{k=1}^{m} sr_k(\Im)}{m} + 0.1\times\left(\frac{1}{m+1}\right)^{\frac{1}{m+1}}, 1\right] \tag{5}$$

In formula 5, multiple routes recommended trust is calculated based on the average of summary single route recommended trust. Moreover, we add a weight parameter as $0.1\times\left(\frac{1}{m+1}\right)^{\frac{1}{m+1}}$ whose value is between 0 and 0.1 to emphasize the importance of recommendation route quantity. While value of m increasing, the weight parameter would increase with it. In like manner, a person would win more trust if he/she gets more recommendations in human society.

Then, we propose the multiple routes recommended trust computation with overlapping routes. Our calculation method is to treat the whole overlapping route as a single route and calculate the multiple parts following the independent route mechanism. We assume that there are two kinds of node in an overlapping route: joint node jd and disjoint node dd. We divide the computation into two steps: calculating the independent multiple routes and calculating the whole overlapping route. The first step aims to remove the disjoint nodes in whole overlapping route and the second step aims to calculate the whole recommended trust as a single route.

Let the overlapping route be expressed by $route = [\Re, jd_1, ..., \Im]$, and the disjoint nodes be dd_q^s which indicates that the disjoint nodes are following joint node jd_q in overlapping route. Then, belief between joint node jd_q and jd_{q+1} can be calculate as following,

$$belief(jd_q, jd_{q+1}) = \begin{cases} belief(jd_q, jd_{q+1}) & no\ dd_q^s\ following\ jd_q \\ mr(jd_q, jd_{q+1}) & else \end{cases} \tag{6}$$

Through formula 6, there would be no disjoint nodes, and overlapping route can be regarded as a single route which is consisted through joint nodes. Therefore, overall recommended trust of overlapping can be calculated as follows,

$$or(\Re,\Im) = sr(\Re,\Im) \tag{7}$$

Here, $dep(\Im) = |route| - 1$ and there is no disjoint nodes in the route.

4.3. Objective Coincidence of Recommended Trust

In human society, people would not make decision for potential selections only depending on other's recommendation information. As a rational decision, a person usually tends to evaluate potential selections with the others' opinions facts. In common sense, if a recommendation obviously departs from the members' trustworthiness realities, the recommendation would be unworthy to believe.

Likewise, it is important and necessary for node to evaluate coincidence between others' impressions and the recommended trust in WSNs.

Let there be demander node $\Re$ and presentee node $\Im$ in recommendation, and there be p different routes for the recommendations. For $\Re$, the objective fact of $\Im$ is the reputation information. Therefore, $\Re$ needs to measure whether the final recommended trust, $rt(\Re,\Im)$, is coincident with its reputation or not in order to realize the trustworthiness of the recommendation.

Assume that there is a neighbor recommender node set, Nd, which includes the neighbor nodes of $\Re$ and each neighbor recommender node nd_i obtains recommended trust, $rt(nd_i,\Im)$ and. Then the objective coincidence of recommended trust can be calculated as follows,

$$coin(\Re,\Im) = \sqrt{\frac{\sum\left[\left(rt(nd_i,\Im)-rt(\Re,\Im)\right)/rt(nd_i,\Im)\right]^2}{|Nd|}}, \quad (8)$$

where $|Nd|$ denotes the total number of neighbor recommender node set. Obviously, the smaller value of $coin(\Re,\Im)$ implies that the recommendation is more trustworthy.

4.4. Optional Degree for Recommendation

By computing the parameters of recommended trust and objective coincidence, demander node have the first-hand impression of presentee node. But these parameters are not sufficient for making decision to select. In human society, people would decide to select a recommended candidate with more rational facts in additional to first-hand information. Consequently, we propose an optional degree for recommendation based on parameters of recommended trust, objective coincidence and other facts.

Let the recommended trust be $rt(d_i,\Im)$ and the objective coincidence of recommended trust be $coin(\Re,\Im)$. Assume that there are p intermediate recommenders d_i in the recommender node set Rd and the presentee node $\Im$ was accepted ξ times and was rejected ω times in past recommendations. Then, the optional degree of presentee node can be calculated as follows,

$$\begin{aligned} &op(\Re,\Im) = \\ &rt(\Re,\Im)\times reputation(\Im)^{\frac{\omega}{\xi}} \\ &\times\left[\frac{\sum_{d_i\in Rd} reputation(d_i)}{|Rd|}\right]^{coin(\Re,\Im)} \end{aligned} \quad (9)$$

In above formula, $|Rd|$ denotes the total number of recommender node set. The value of $reputation(\Im)$ is impacted by accepted time ξ and rejected time ω. The more accepted times and the less rejected times occurred for $\Im$, the value $reputation(\Im)^{\frac{\omega}{\xi}}$ would be larger. Likewise, in formula 9, $coin(\Re,\Im)$ indicates that whether recommender nodes' recommendation is honest and accords with objective fact or not, while the average of recommender's reputation indicates the whole credit of recommenders. Therefore, the factor is more optional while average of recommenders' reputation is larger and $coin(\Re,\Im)$ is smaller.

4.5. Proposed Framework

Generally, people would not trust strange one depending on just one recommender. In order to ensure the presentee's reliability, people may inquire the trustable facts from multiple recommendation sources. Likewise, node should consider trust degree of $\Im$ from multiple recommendations in WSNs. Therefore, we propose a recommendation trust computation framework (RTCF) for recommended trust evaluation.

Definition 5. A recommendation trust computation framework for WSNs can be defined formally as following,

$$\Theta = (\Re,\Im,D,Route,Acceptability), \quad (10)$$

where, $\Re$ and $\Im$ denote the recommendation receiver and the presentee respectively, $D=(d_1,...,d_n)$ denotes the recommenders, $Route$ is a set of vector as $route_k=[d_1^k...]$ which denotes the recommendation routes from $\Im$ to $\Re$, and $Acceptability$ denotes the acceptable degree of $\Im$ which consists of three parameters, $rt(\Re,\Im)$, $coin(\Re,\Im)$ and $op(\Re,\Im)$. $rt(\Re,\Im)$ is the recommended trust from $\Im$ to $\Re$ through single route sr or multiple routes mr. $coin(\Re,\Im)$ is the matching degree between recommendation and reputation of $\Im$ to measure whether the recommended trust of $\Im$ is coincident with its reputation. $op(\Re,\Im)$ denotes a qualification degree whether the presentee can be trusted or not.

5. Proof of Correctness

In this section, we present a set of lemmas and theorems for our recommended trust computation in order to prove the correctness.

Lemma 1. In WSNs, trust can be conditional transmitted between nodes in recommendation.

Proof. Generally, trust does not have the character of transitivity [15]. But in recommendation, trust can be transmitted in some conditions, which was addressed in [4].

1) Intermediate recommenders explicitly communicate their trusts in presentee to demander, as a 'recommendation'.

2) Demander trusts recommenders, i.e. recommender trust exists in the system.

3) Demander is allowed to make judgments about the 'quality' of recommendation (based on demander's policies).

4) Trust is not absolute, i.e. demander may trust presentee less than recommender does, based on recommender's recommendation.

In our paper, nodes can explicitly communicate their trust as recommendation. And intermediate nodes do exist in WSNs. Moreover, demander can judge the recommendation based on its willingness, and the recommended trust obviously dumps in recommendation in our proposed formulas. Hence, trust can be transmitted conditionally in recommendation.

Lemma 2. In WSNs, all nodes can hold the recommended trust information from different intermediate recommenders about presentees so that the case of multiple intermediate recommenders is available.

Proof. For each node in WSNs, it can hold past transactions, including recommendations because it can generate and renew subjective belief with other nodes. Therefore, while a node receives a recommended trust, it would hold such recommendation as first impression about a strange node. Thus, every node has potential to deliver its recommendation to others and become an intermediate recommender. Lemma 2 holds its correctness.

Theorem 1. Recommended trust in RTCF computation reflects both objective and subjective judgments about pressentee.

Proof. According to lemma 1, demander node is allowed to make judgment about the recommendation based on its own policies. Then, the recommended trust indicates the subjective judgment of demander node. At the same time, formula 3, 4 and 5 shows that such judgment of demander node is based on trust information of belief and reputation. Hence, recommended trust is calculated from both subjective and objective aspects.

Theorem 2. Spurious recommendation from malicious recommender nodes is identifiable for demander node in RTCF.

Proof. According to formula 2, it is impossible for a malicious node to win a high reputation since the reputation reflects the whole members' opinions in WSNs. In case a malicious node is a recommender in recommendation, demander node would get a lower $sr(\Im)$ or $mr(\Im)$ through formula 4 and 5 because of low reputations of $reputation(d_i)$. On the other hand, if a spurious presentee node is recommended by others, the value of $coin(\Re,\Im)$ or $op(\Re,\Im)$ would be low through formula 8 and 9 because of the low reputation of $reputation(\Im)$. Moreover, theorem 1 shows that recommended trust is evaluated from both subjective and objective aspects. Then, demander node would not get high recommended trust value based on low reputations of malicious nodes.

6. Example and Examination for RTCF

6.1 Example

In this section, we proposed an example to explain the efficiency of our recommended trust framework. In our scenario of example, we set a recommendation between demander node $\Re$ and presentee node $\Im$. There were nine intermediate recommender nodes which composed three recommending routes between $\Re$ and $\Im$. Route I was an overlapping multiple routes composed by recommender node 1, 4, 5 and 8. Route II and III was single routes composed by recommender node 2, 6, 9 and node 3, 7 respectively. The recommendation is shown in Fig. 1 as following.

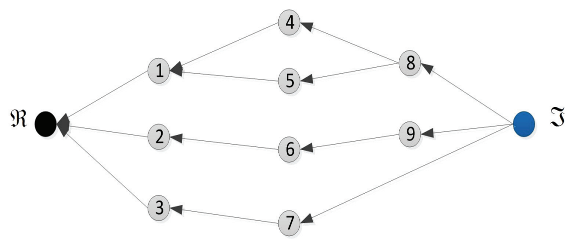

Fig. 1. Example of recommended trust.

We set the trust information of belief and reputation about the nodes in Table 1 and Table 2.

Based on computation method of RTCF, parameters of recommended trust, objective coincidence and optional degree were calculated as following (Table 3).

Table 1. Belief between Nodes.

Node	Belief	Node	Belief
$\Im\rightarrow 9$	0.75	$6\rightarrow 2$	0.95
$\Im\rightarrow 8$	0.95	$5\rightarrow 1$	1.0
$\Im\rightarrow 7$	0.8	$4\rightarrow 1$	0.9
$9\rightarrow 6$	0.9	$3\rightarrow \Re$	0.75
$8\rightarrow 5$	0.95	$2\rightarrow \Re$	1.0
$8\rightarrow 4$	0.65	$1\rightarrow \Re$	0.8
$7\rightarrow 3$	0.8		

Table 2. Reputation of Nodes.

Node	Reputation	Node	Reputation
$\Im$	1.0	5	1.0
1	1.0	6	0.65
2	0.9	7	0.9
3	0.95	8	0.75
4	0.7	9	1.0

Table 3. Parameters of RTCF.

	Parameters
8→1	$belief(1,8) = 0.663$
Route I	$or_I(\Re,\Im) = 0.52$
Route II	$sr_{II}(\Re,\Im) = 0.582$
Route III	$sr_{III}(\Re,\Im) = 0.581$
Recommended trust	$rt(\Re,\Im) = 0.632$
Objective coincidence	$coin(\Re,\Im) = 0.07$
Optional degree	$op(\Re,\Im) = 0.626$

Compared with each route of recommendation, the whole recommended trust is larger because more recommenders imply more trustable recommendation. And also, while recommended trust is quite deviating from the presentee node's reputation, the coincidence value would be larger and optional degree value would be less.

6.2. Examination

In this section, we examine our proposed trust management method through a series of simulations. We performed our simulations on the NS-3 simulator [17] which allows the simulation of wireless networks. For initial setting, we deployed 300 nodes in simulator. As initial setting, reputation values of honest nodes followed a normal distribution with mean 0.8 and variance 0.1 and reputation values of malicious nodes were set between 0.2 and 0.8 at random. The network topology was generated at random and average out-degree of a node was 4. Nodes which had a direct link between them could execute transactions by default. Then, we set initial past working data, including past judgments and working capacities, for nodes according to their honest and malicious identities and allowed nodes to query the past data from their neighbor nodes at any time.

In first examination, we aimed to testify the efficiency of recommended trust computation. We assumed that there were not malicious nodes in our simulation. For all users who received recommendation, they must accept and transmit it to their neighbors while recommended trust value satisfied $recommend(\Re,\Im) \geq 0.75$. We set three groups as follows: Baseline1 used the EigenRep method, which was given in reference 12, to calculate the trust relationships among users and decided whether transmitting the information or not according to the direct recommender. Baseline2 used the belief and reputation computation methods in this paper. All users decided whether transmitting information or not based on the average of belief and reputation. Baseline3 used the recommended trust computation in SRTCF to measure whether information could be transmitted. We repeated 100 times of recommendation dissemination and recorded the average dissemination depth of above three groups, which was shown in Fig. 2 as follows.

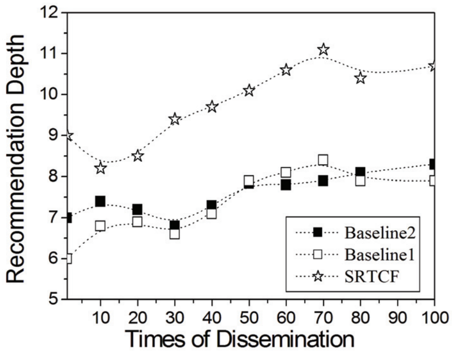

Fig. 2. Average dissemination depth of recommendation.

In second examination, we introduced malicious nodes whose reputation were lower than 0.2 and we appointed them to release fake recommendation. We defined that a malicious recommendation was the one which satisfied the condition $(recommend(\Re,\Im) \geq \alpha) \wedge (optional(\Theta) \geq \beta)$. We set three groups in this examination and the thresholds of $<\alpha,\beta>$ were set as $<0.7,0.8>$, $<0.8,0.85>$ and $<0.8,0.9>$ respectively in group 1 to 3. We repeated 50 times of recommendation dissemination in three groups under different percent of malicious users. With the increasing of malicious users, the percent of malicious recommendations which were identified accurately were shown in Fig. 3. As shown in Fig. 3, we can see that percent of identified malicious recommendation increased with the enlargement of thresholds in three groups. That means our method can avoid the malicious recommendation effective.

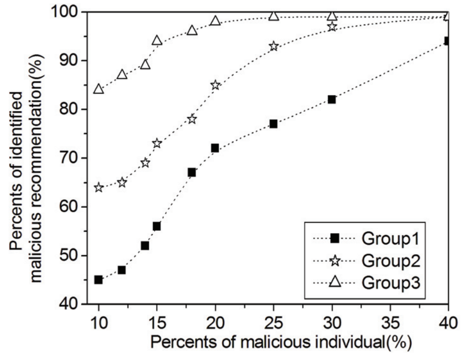

Fig. 3. Malicious recommendation identification with RTCF.

7. Conclusion

Security is very important for WSNs because of the relax-coupled network environment. Existing researches proved that trust is a feasible to cope with this challenge. In this paper, we introduced subjective and objective trust to build up a recommended trust computation for strange nodes so that they could get indirect trust through recommenders. We proposed notions of belief and reputation to evaluate the subjective trust relationships and the objective trust view for nodes. Then, we addressed the recommended trust notion based on above two trust notions. In our paper, recommended trust is calculated through single route or multiple routes between recommendation demander and presentee. Moreover, we presented two parameters of objective coincidence and optional degree for recommendation. Further, we proposed a recommended trust computation framework (RTCF) for WSNs nodes. Finally, lemmas and theorems were presented in order to prove the correctness RTCF. We plan to testify the efficiency of our work in several simulations or applications in near future.

Acknowledgements

We thank National Natural Science Foundation of China (61103069 and 71171148), Innovation Program of Shanghai Municipal Education Commission (13YZ052), the Shanghai Committee of Science and Technology (11DZ1501703 and 11dz1210601)， the Program of Shanghai Normal University (DCL201302), National High-Tech Research and Development Plan of China (863)(2012BAD35B01 and 2012AA062203)， the National Social Science Research Foundation of China (12CYY031), the Ministry of Education of China (12YJC740082) and Natural Science Fund of ShangHai Normal University (No. SK201221) for supports.

References

[1]. A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, *Communications of the ACM*, Vol. 47, 2004, pp. 653-657.

[2]. A. Boukerch, L. Xu, K. El-Khati, Trust-based security for wireless ad hoc and sensor networks, *Computer Communications,* 30, 2007, pp. 2413–2427.

[3]. Lei Huang, Lei Li, and Qiang Tan., Behavior-Based Trust in Wireless Sensor Network, *APWeb Workshops, LNCS,* 2006, 3842, pp. 214 – 223.

[4]. Alfarez A. Rahman, Stephen Hailes, A distributed trust model, in *Proceedings of the 1997 Workshop on New Security Paradigms*, 1997, pp. 48-60.

[5]. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, Wireless sensor network survey, *Computer Networks,* Vol. 52, 2008, pp. 2292–2330.

[6]. P. Dewan, P. Dasgupta, Securing P2P networks using peer reputations: is there a silver bullet, in *Proc. IEEE Consumer Communications and Networking Conference*, Las Vegas, US, 2005.

[7]. Z. Liu, A. W. Joy, R. A. Thompson, A dynamic trust model for mobile ad hoc networks, in *Proceedings of the 10th IEEE International Workshop Future Trends Distr. Comput. Syst.,* Suzhou, China, May, 2004, pp. 80-85.

[8]. A. A. Pirzada, C. McDonald, Establishing trust in pure ad-hoc networks, in *Proceedings of the 27th Conf. Australasian Computer Sci., ACM International Conf. Proc. Series,* Dunedin, New Zealand, 2004, pp. 47-54.

[9]. S. Buchegger, J. L. Boudec, Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks, in *Proceedings of the 10th Euromicro Workshop Parallel, Distributed and Network-based Process,* 2002, pp. 403-410.

[10]. P. Michiardi, R. Molva, Core: A collaborative reputation mechanism to enforce node cooperation in mobile AD HOC networks, in *Proceedings of the Sixth IFIP Commun. Multimedia Secur. Conf.,* Portorosz, Slovenia, 2002, pp. 107-121.

[11]. Audun Jøsang, Roslan Ismail, Colin Boyd, A survey of trust and reputation systems for online service provision, *Decision Support Systems,* Vol. 43, Issue 2, March, 2007, pp. 618-644.

[12]. A. Abdul-Rahman, S. Hailes, Supporting trust in virtual communities, in *Proceedings of the 33rd Ann. Hawaii International Conf. Syst. Sci.,* 2000, Vol. 6, pp. 6007-6016.

[13]. Raphael Yahalom, Birgit Klein, Thomas Beth, Trust Relationships in Secure Systems - A Distributed Authentication Perspective, in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 1993.

[14]. J. Liu, V. Issarny, Enhanced reputation mechanism for mobile ad hoc networks, in *Proceedings of the 2nd International Conference on Trust Management*, Vol. 2995, March 2004, pp. 48-62.

[15]. Audun Jøsang, The right type of trust for distributed systems, in *Proceedings of the New Security Paradigms '96 Workshop*, 1996.

[16]. S. Buchegger, J. Boudec, A robust reputation system for P2P and mobile ad-hoc networks, in *Proceedings of the 2nd Workshop the Economics of Peer-to-Peer Systems*, Cambridge, US, June 2004.

[17]. NS-3, <http://www.nsnam.org/index.html>.