A Comprehensive Trust Model Based on Reputation and Fuzzy Theory

Xianghe Wei
School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China
School of Computer Science and Engineering, Huaiyin Normal University, Huaian, China
Email: wxh@hytc.edu.cn

Hong Zhang, Xuan Mo, Yong Qi, Zhen Liu and Qianmu Li
School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China
Email: zhhong@mail.njust.edu.cn, markmo_cs@163.com, qyong@njust.edu.cn,
xyzliuzhen@qq.com, liqianmu@126.com

***Abstract*—In Ubiquitous Network, the core problem is how heterogeneous terminals communicate credibly between each other. We will achieve communication and "Ubiquitous" between varieties of heterogeneous terminals only if more reliable interaction through heterogeneous terminals could be made. This paper puts present a Comprehensive Trust Model based on Reputation and Fuzzy subsystems (CFMBRF), indirect recommending trust calculation method of the model adopts the "an fuzzy based credibility evaluation method for indirect trust computation", then on the basis of the model based on reputation, import the fuzzy inference subsystems, it is able to handle subjective concept such as " importance of a interaction", "the decisions in the uncertainty region " and "setting the result of interaction ", can humanistic make decision about uncertain problem. This paper simulates the network having no-fuzzy subsystem and network which have the fuzzy subsystem, makes comparison between the two networks, tests overhead and stability of the CFMBRF. It can be seen that the network using the fuzzy subsystem greatly increased the validity of the interaction, decreased the number of query for the reputation vector, and proved the effectiveness of the CFMBRF model.**

***Index Terms*—Ubiquitous Network, Fuzzy inference, Trust mechanism, Reputation**

I. INTRODUCTION

The universality of Ubiquitous Network produced a series of basic safety issues, such as trust, confidentiality and privacy. As a result, "computing trust" emerged as a new field [1] . The concept of "trust" comes from sociology which makes the model of reputation and trust very difficult to design. A trust model based on the reputation and the self-confidence put forwarded by Ramchurn et al in literature [3], processes history interactions using certain degree of fuzzy logic. In the model, self-confidence is derived from the direct interaction between the interactive nodes while reputation is derived from the indirect interaction and information collected from other nodes in the network. In literature [4], Schlager et al use fuzzy cognitive map and trust vector to proceed the reputation management based on authentication mechanism and authorization infrastructure. In literature [5], Schmidt et al propose a fuzzy theory based framework to make the optimal choice. Also, in literature [6], Schmidt et al propose a customizable fuzzy theory based trust model which incorporates the historical interaction, such as interaction reviews and adjusting credibility. In literature [7], A. Tajeddine et al present a reputation model based on reputation, but when the last few reputation values fall into the grey area, processing is not ideal.

Recommendation service only provides a single trust value (to be obtained by the interaction with the nodes for assessment) as recommendation in the present trust model. But this single recommendation trust value provided by presenter represents its subjective view of the unknown entity, not well reflecting the level of trust under certain circumstances. For instance, S requires recommendation on unknown entity C and receives responses from presenter A and B, recommendation values are TA=3.5, TB=2.5, respectively. Does this mean they should be given the same weight in the calculation of polymerization recommendation trust? Assume that, T_A is obtained with a time t_A and T_B is with a time t_B, t-current-tA > tcurrent-tB, in the past interactions with C, A has less interaction history then B. Apparently, the recommendation provided by B is more reliable than A when assessing the reputation of C, because B is closer and has more interaction experience. Additionally, if the interaction between B and C is more sensitive than A and C in the context of interaction, it will further strengthen the credibility of B's recommendation. In order to solve this problem, an effective indirect trust calculation method is introduced in this paper.

Although there are now trust based trust model, building trust path is still not suitable in the Ubiquitous Network due to the huge overhead caused by instantaneous and uncertainty of the nodes in Ubiquitous Network. This paper puts present a Comprehensive Trust Model based on Reputation and Fuzzy Theory CFMBRF (Comprehensive Trust Model based on Reputation and

doi:10.4304/jcp.9.11.2666-2676

Fuzzy subsystems). CFMBRF is an improved reputation-based trust model, taking into account the various important factors in reputation value calculation, such as, direct experience, reputation value, credibility of recommendation, reputation value decay based on dynamic decay factors, the first impression and mixed recommendation by the terminals to decide whether the terminal is creditable and can be interacted with or not.

The rest of the paper is organized as follows. In section 2, we outline the design of the reputation. In section 3, we introduce the design of the fuzzy subsystem. Section 4 describes the whole procedure of the CFMBRF model. Section 5 presents the simulation experimental results of the model. And, we give the conclusion in section 6.

II. The Design Of Reputation

A. Direct Trust

(a) Initialization

(b) A new ubiquitous node may be added into Ubiquitous Network at any time due to its dynamic nature. To consider a special case, the terminal Z is a newly added ubiquitous node in the system. Other terminals in the system will give Z an initial test phase, in the phase, some useless data which they know the results and the completion time will be sent to Z. In this stage, the terminal will continually calculate the reputation value of Z, check its credibility until the reputation information stabilizes then the value of the first impression FI will be set to the stabilized reputation value. Each terminal will have its own test period to test the credibility of Z. And Z can't guess the length of the test period, because once Z knows the duration, Z can interact friendly for the duration but become dishonest when gain other terminals trust. On the other hand, if one terminal Q do not want to wait till the end of the test period, it can give Z a random FI (First Impression) value according to its own preferences.

$$\mathrm{repY/X(0)} = \mathrm{first\_impression} \quad (1)$$

(c) reputation value calculation

(d) In order to ensure the real-time accuracy of the reputation value of the nodes in the Ubiquitous Network, the interaction results will be calculated by the RI fuzzy subsystem and then back to the source node X. At last, X need to recalculate the reputation value of Y according to formula (2):

$$\mathrm{repY/X(0)} = \xi \times \mathrm{repY/X}_{before\_int} + (1-\xi) \times RI \quad (2)$$

Where RI is the result of the interaction perceived by X and its range is the same as the reputation value. ξ is a parameter within range [0.1 -0.3]. It will give a higher weights to the reputation of the interaction just happened while give lower weights to the ones occurred long before. $\mathrm{repY/X}_{before\_int}$ is the reputation value of X to Y before the interaction. The detailed description of the formula can be found in literature [8].

B. Indirect Trust

According to the character of the ubiquitous network, the indirect trust is divided into three kinds: the neighbor nodes indirect trust, strange nodes indirect trust and trusted nodes indirect trust. Neighbor nodes, strange nodes and trusted nodes will only be checked for one time in practice to get recommendation reputation values to deduce the comprehensive trust value. Because not using the method of trust path, the time and resource overhead it takes to establish the trust path decreases.

For neighbor nodes indirect trust and strange nodes indirect trust, CFMBRF adopted the indirect trust calculation method described in chapter 3.

For trusted nodes, recommendation credibility can be calculated by the trust degree of recommendation requester to the node X_i, as certain trust relationship has been established between recommendation requester and the presenter. The formula is as follows:

$$T_{trusted} = (\sum_i t_i repY / X_i) / \sum_i t_i \quad (3)$$

Where $repY / X_i$ represents the reputation value node X_i to target node Y. t_i is the credibility of source terminal to node X_i.

C. Comprehensive Trust

Comprehensive trust means aggregating recommendation trust and direct trust to get the comprehensive trust value of the target node.

$$\begin{aligned} & repY / X_{before\_int} \\ & = A \bullet repY / X + B \bullet T_{neighbor} + C \bullet T_{trusted} + D \bullet T_{strangers} \\ & = A \bullet repY / X \\ & + B \bullet (\sum_i \alpha_i repY / X_i) / \sum_i \alpha_i \\ & + C \bullet (\sum_j \beta_j repY / X_j) / \sum_j \beta_j \\ & + D \bullet (\sum_l \delta_l repY / X_l) / \sum_l \delta_l \end{aligned} \quad (4)$$

Where, $\mathrm{A+B+C+D=1}$, $\mathrm{A、B、C、D} \in [0,1]$, A represents direct trust weight factor, B, C, D represent the weight factors of neighbor recommendation trust, trusted node recommendation trust and strange node recommendation trust respectively. α_i、β_j、δ_l represent the credibility Cr of neighbor node to terminal Y after fuzzy calculation, the credibility of source terminal to trusted node X_j, the credibility Cr of strange node to terminal Y after fuzzy calculation respectively. From the social relationship point, the sense of trust obtained from direct interaction is higher than indirect interaction when nodes interact with each other, therefore, with the increase in the number of network interactions, recommendation request nodes are more willing to believe the direct

interaction trust degree with the target node. Reputation range is [0, k], therefore, $0 \le \text{repY/X} \le \text{k}$.

Now two thresholds must be determined in the system: θ and φ, represent complete trust threshold and complete not trust threshold respectively.

If $\text{repY}/\text{X} \ge \theta \rightarrow$ Y is credible.

If $\text{repY}/\text{X} \le \varphi \rightarrow$ Y is incredible.

If $\varphi \le \text{repY}/\text{X} \le \theta \rightarrow$ using fuzzy inference method.

D. Decay Coefficient τ

Over time, if there is little or no interaction occurs, the reputation value of terminal Z to terminal Y will attenuate according to formula (5):

$$repY/Z(t) = final\_value + (initial\_value - final\_value)e^{(t-t_0)/\tau} \quad (5)$$

In which, τ is the decay coefficient determining the decay level of reputation information, t_0 is the last time when Z calculates the reputation value of Y. final value represents, with the passage of time, and no interaction occurs, the convergence value of reputation value to the terminal Y. initial value is the reputation value when t=t0 .

Each terminal keeps a decay coefficient for other interactive terminals. τ_Y is a dynamic decay coefficient to terminal Y. The coefficient would be a normal value initially, then it will change when the reputation value of Y changes (between the maximum and minimum value defined previously).

Calculating the degree of difference $D = New - Old$

If $|D| \le 1$, then $\tau_Y = \tau_Y \times round(5 - 4 \times |D|)$

If $D > 1$, then $\tau_Y = \dfrac{\tau_Y}{2 \times round(D)}$

If $-D > 1$, then $\tau_Y = \tau_Y \times round(|D|)$

Limiting the new value of τ_Y in range $[\tau_{\min}, \tau_{\max}]$

In which, k=5, τ_{min}=1000, τ_{mxa}=10000. Old represents the reputation value of Y before this interaction, New represents the reputation value after this interaction.

TABLE I

TERMINAL TRUST TABLE

HostID	192.168.1.105
Status	Neighbor
Weighting Factors	0.7
Reputation value	3.7
Decay factor	5230
nt	30
SS	0.11
Int_with	43
Att	72

E. Colleting/Saving Reputation Value

Each terminal keeps a table like Table 1. This table holds the records of other terminals like this: HostID is an identification ID, it can be an IP, a URL, etc.; Status is the status of a neighbor, a friend or a stranger; Weighting Factors represents the credibility of HostID (α, β or δ). Decay factor is the decay factor τ_i; t is the time when reputation value be recorded; nt represents the number which table held terminal interacts with the corresponding terminal of the HostID; SS is the sensitivity of the presenter; Int_with is the number of completed interactions(passive interaction) the terminal interacts with other terminals within a time interval TI; Att is the number which other terminals attempted to interact with the terminal within a time interval T1.

Reputation vector is just a subset of the reputation table which contains ID, reputation value, nt, the number of interactions within last interval TI, the sensitivity of presenter SS, the time of last interaction t. But terminal X would not check reputation vector for more than once within an interval. Additionally, terminal X would only check terminals whose cooperation value within the cooperation threshold. The cooperation value of terminal M would be thought as inaccurate and M would be checked if the number of attempts of M bellows a certain threshold. Meanwhile, when the number of attempts exceed the threshold, terminal X would get enough information to calculate a reasonable cooperation value for M. The procedure is as Fig. 1.

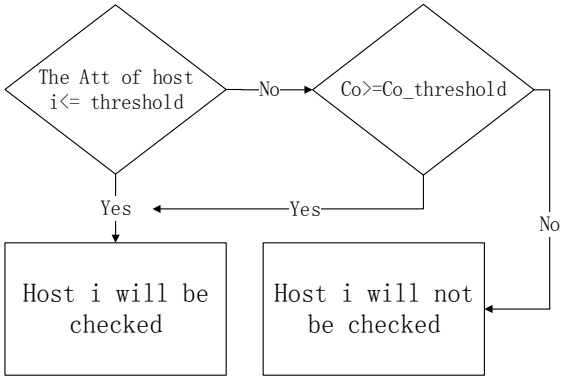

Figure 1. Checking terminal base on cooperation degree.

But whenever been checked, τ_i will be used to decay the reputation value by the terminals and reputation vector will be sent to X. Terminal x will calculate the reputation weight factor, reputation value and decay factor etc. Then, check the reputation value Y and determine interact with Y or not.

(1) time interval TA

X only collects reputation vector for once for reputation vector have a very small change in the time interval TA. TA is a value predefined by each terminal according to the different needs for real-time data.

(2) cooperation value Co

Cooperation Co reflects a terminal's willing of cooperation and the willing of providing service for other terminals. The cooperation value of Y to X is calculated as follows:

$$Co(Y/X) = \frac{Int\_with_Y}{Att_Y} \quad (6)$$

In which, Co is in the range of [0, 1]. Co will decrease the times of checking reputation vector; and, to uncooperative terminals, it also saves the bandwidth and waiting time. Int with Y is the number of completed interactions (passive interaction) terminal Y performed with other terminals within the previous time interval T_1; AttY is the number of interactions other terminals attempted to establish within the previous time interval T_1.

III. The Design Of Fuzzy Subsystem

The maximum threshold of terminals to be checked was settled In CFMBRF. With the increase of the threshold value, the waiting time for gathering reputation information would become longer and the size of communication checks and reputation information would become bigger. Thus, it would have huge impact on the total time of interaction and bandwidth consumption.

If the interaction is critical, initial terminal would spend more time to ensure the target terminal is credible. Therefore, more terminals would be checked for the reputation value of the target to ensure the credibility of the target and get a smaller first impression value (FI).

On the other hand, when the interaction is not critical but needs fast response, the terminal would trust others more easily. Therefore, it will increase FI and decrease the number of terminals to be checked.

This means that the initial terminal has to weigh the security time based on the importance of the transaction. So, when a terminal only checks part of the terminals, to check which part become a problem. In this case, the initial terminal compares the weight of his neighbor friends and the strangers: $B\alpha, C\beta$ and $D\delta$ (α, β, δ is the corresponding credibility of each recommendation when calculating the comprehensive trust in the last time), and, it will interacts with the terminal which has the highest weight. This will produce a dynamic hierarchy for the terminal, friend nodes (have higher β value) may be more credible then neighbor nodes.

A. Importance Logic

Importance mainly depends on three factors. The first is the monetary value (i.e., the resource consumption of the service provider for the interaction). The transaction will be considered as critical and important when monetary value is very high and not so important when monetary value is very low.

The second is the criticality of the result of the transaction. With the increase of the criticality level, the result is more important and necessary. And this requires to have fewer risks. So a high importance factor should be given. Similarly, the lower criticality, the lower importance.

The third is the time for getting the result. The total interaction time is a basic problem which has negative effects on importance level. On the one hand, fewer terminals need to be checked for the reputation value of the target terminal if fast obtaining is request, therefore, the interaction will has a lower importance value. On the other hand, when interaction time is not critical and the result is not acquired quickly, the interaction will get a higher importance value.

In the Importance fuzzy subsystem, the criticality of monetary value and interaction results are divided into three level: low, medium, high. The time needed is divided into two kinds: fast and slow. And the importance level is divided as: low, medium, high.

B. Gray Region Decision

Whether the reputation value in the gray area is credible or not? In which, the reputation value is between the complete trust threshold and the complete mistrust threshold. In order to solve this problem, a fuzzy subsystem is introduced to process when to interact or not. In that case, interaction decisions are more subjective, because, at certain reputation value, a terminal will interact with the target terminal while the other doesn't.

The fuzzy decision in the gray area is mainly depends on three factors. The first is the character of a terminal. When the source terminal becomes more credible, even if it has little doubt, it will still give priority to interact with the target terminal. But when the source terminal becomes more paranoid, it tends not to interact unless it can be guaranteed to be a good interaction and the target terminal has a good purpose.

The second is the concept of importance fuzzy factor defined previously. When the interaction becomes more important, that is, the data is more critical or the monetary value of the transaction is higher, nodes will tend not to interact unless a good interactive result is guaranteed. But when the importance of interaction decrease, that is needing to get the result very quickly or the importance and monetary value of the interaction is very low, nodes tend to interact without a guaranteed good result.

The last factor is reputation value of the target value, and it's the most important factor for make decision. Because, a target terminal whose reputation value tends to the credible threshold θ is more likely to be a good node than the terminal whose reputation value tends to incredible threshold φ.

The three factors are combined to be calculated to decide whether to interact or not. In the FDecision subsystem, the character is considered as credible or paranoid, importance and the fuzzy reputation value is divided into three levels: high, medium, low.

C. RI (Result of Interaction) Calculation

The final fuzzy subsystem was proposed to calculate the value of the result of interaction (RI) in CFMBRF. Also, this value is subjective: when an interaction is considered to be a good one or a bad one, the levels of satisfaction of the initial terminal is not clear yet. But a

decision made by a terminal will have impact on the reputation value of the target terminal, furthermore, will influent the whole system. So, the fuzzy subsystem is for settling a subjective standard for judge whether an interaction is good or not uniformly, at the same time, keeping the relative inference of each terminal.

The value of RI depends on three factors. The first is the accuracy of the result and it is determined by judging whether the result of interaction meets expectation. When the accuracy is high, the result will be considered as a good one, and the value of RI will be higher. But when an interaction is considered to be a bad one, the value of RI will become lower.

In the RI subsystem, the result of an interaction could be good or bad, the time of interaction could be fast, slow or equivalent, predefined monetary value could be high, medium or low.

IV. The Whole Procedure Of The CFMBRF Model

Fig. 2 explains the event flow of CFMBRF model. When terminal X wants to interact with terminal Y, X first use importance fuzzy inference subsystem to calculate the importance of interaction with Y. Then, X counts the time passed from the last query of reputation vector, if it is bigger than the predefined time interval Ta, X will decide how many terminals to be checked for calculate the reputation value of Y at most. The number is the upper limit of terminals to be queried, in case of too much query get in the network.

After that, to terminals whose cooperation value are bigger than the cooperation threshold, terminal X will check for their reputation vectors. The terminals been queried will get their reputation value decay, then, they will send their reputation vector to X, and X will calculate the weight of indirect recommendation and the cooperation value of the terminal. Terminal X will decay its old reputation value then present information and calculate the comprehensive reputation value of terminal Y according to formula(4). If the time passed from the last query of reputation vector to present time do not exceed Ta, X will directly decay its old reputation value and skip the middle steps.

After the comprehensive reputation value have been calculated, terminal X need to make a choice: if the reputation value of Y is less than the complete mistrust threshold, then Y is incredible, X will not interact with it; if the reputation value of Y is bigger than the complete trust threshold, Y is credible, and X will interact with it; but if the reputation value of Y is between the two thresholds, terminal X will use FDecision fuzzy inference subsystem to see whether Y is credible or not.

After the interaction, X will calculate the interaction result RI which is the quality index to measure the result of the interaction. RI is calculated through the fuzzy inference subsystem. At last, terminal X will use RI to recalculate repY/X according to formula (2) and calculate the new decay coefficient to Y based on the interaction result difference terminal Y has with the previous result.

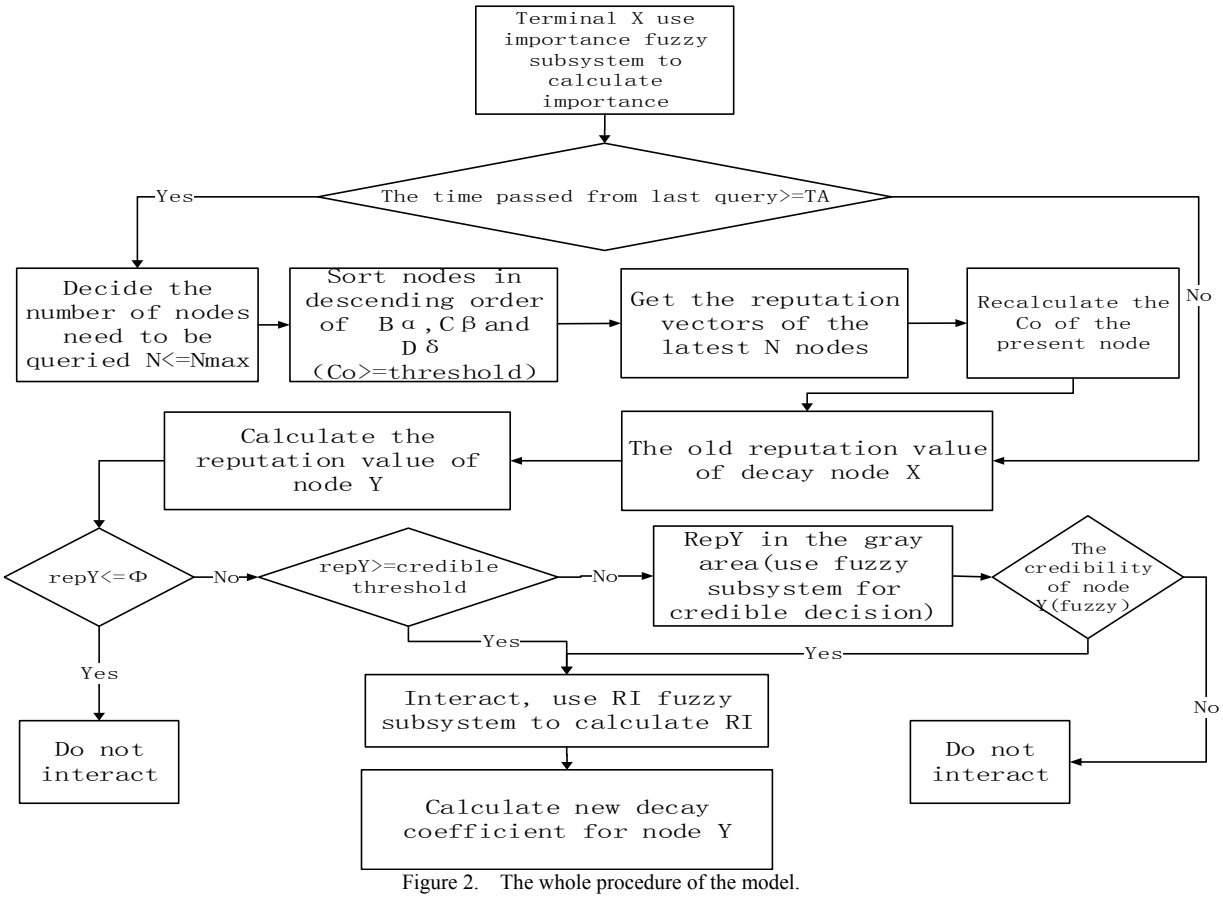

Figure 2. The whole procedure of the model.

Table 2 makes a comparison between the CFMBRF model and some current mainstream models and analyzes their features.

TABLE II
THE COMPARISON BETWEEN CFMBRF MODEL AND SEVERAL OTHER MODELS

	[3]	[4]	[5]	[6]	[7]	[2]	CFMBRF
Mixed reputation calculation			YES		YES	YES	YES
The location of the network members					YES	YES	YES
Interaction history information	YES	YES	YES	YES	YES	YES	YES
Trust propagation	YES	YES	YES	YES	YES	YES	YES
First impression					YES	YES	YES
The result of interaction	YES	YES	YES	YES	YES	YES	YES
Fixed decay factor					YES		YES
Dynamic decay factor					YES	YES	YES
Gullible type or paranoid type					YES		YES
Cooperative degree					YES		YES
The number of interactions					YES		YES
Dishonest recommendation filter							YES
Fuzzy theory	YES	YES	YES	YES			YES

Notes: “mixed reputation calculation” indicates that the aggregate calculation of comprehensive trust takes the recommendation of neighbor node, credible node and strange node into account; ”the location of the network members” value model considers the location of terminals in network, for instance, the nodes within the communication range of A is the neighbors of A; “interaction history information” represents the history information of the interactions between terminal nodes; ”reputation propagation” refers to the initial reputation value of a newly added node which other nodes defined. ”The result of interaction” is the quality of sensed interaction, the range is same as reputation value; “gullible or paranoid type” refers to the features of terminal node, paranoid node may be very persistent on its own security and it will interact with the node who is definitely honest or has a very high reputation value, on the other hand, gullible terminal accept the interaction, only needs the reputation value of target nodes is in an acceptable range; ”cooperative degree” is the ratio of the number of interactions terminal node accepted and other nodes attempted to establish; “dishonest recommendation filter” indicates to filter out some dishonest recommendation, such as, a terminal node with a very high reputation value gives a pretty low recommendation reputation value when present to other nodes, vice versa.

V. SIMULATION EXPERIMENT

In order to evaluate the whole trust model and prove its effectiveness and reliability in Ubiquitous Network, a network with 10 terminals which can interact randomly was simulated by VC++. As Fig. 3 shows, the network contains 5 traditional network nodes which could be laptop, PDA, PC or server; 2 sensor network nodes (SNN); and three WIFI network nodes which moved dynamically in the WIFI area.

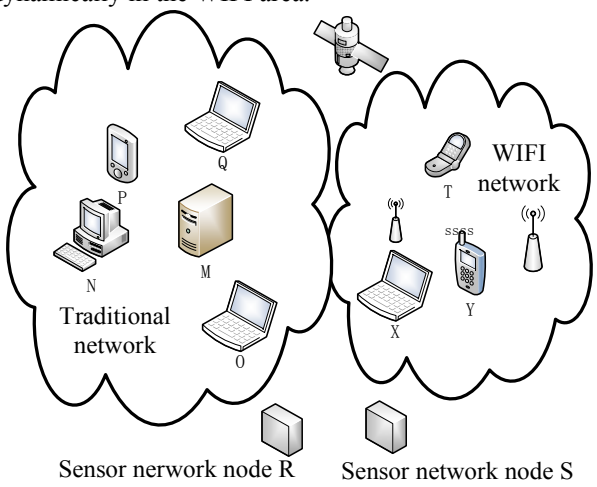

Figure 3. The simulation structure of Ubiquitous network

There was only one interaction in any simulation cycle. The reputation value changed from 0 to k=5. An interaction was incredible when the reputation value was below $\phi = 1$, and if the reputation value was over $\theta = 4$, the interaction was credible. If the reputation value was in the gray area between ϕ and θ, the model would use FDecision subsystem to decide if it is credible or not. On the other side, whether it was credible or not was decided by the bias possibility of reputation value of ϕ and θ in no-fuzzy systems. In the simulation, terminal X and Y was settled to be terminals having a bad reputation, the interaction reputation value they gave was randomly distributed between 0 and ϕ, other terminals were terminals having good reputation and the reputation value they gave is between θ and k. Table 3 shows some constants in the simulation. All terminals were considered as neighbor terminals within the same surveillance area. Therefore, weight factors C and D were need less. The first impression value was defined as FI=2.5 and the initial decay factor was defined as $\tau_0 = 5000$.

The three fuzzy subsystem, Importance, FDecision, RI, were designed and realized by the fuzzy tool case in

MATLAB combined with some C++ code. The system made comparison between terminals which had good reputation and bad reputation, meanwhile, made comparison between the ratios terminals with a good reputation interacted with terminals with a bad reputation. Additionally, we compared a how many terminals had been checked for the reputation value by a certain terminal.

TABLE III
SOME SIMULATION CONSTANTS IN COMPREHENSIVE TRUST MODEL

parameter	value
A	0.55
B	0.45
Φ	1
FI	2.5
τ_0	5000
τ_{min}	1000
τ_{max}	10000

A. The System Simulation of No-fuzzy Logic

In order to prove the effectiveness of the fuzzy subsystem, we first simulated the network without any fuzzy subsystem, then introduced the fuzzy subsystem and compared both of them at last.

The result of the simulation showed that the reputation value of terminal M to terminal O who had a good reputation is in a rising trend, and it would gradually settled in the complete trust area , only the first attempt is a mistrust behavior. In the first attempt, the reputation value of M to O is 3.8 falling in the gray area and terminal M determined not to interact with terminal O according to probability. Thus, terminal M thought good terminal O as credible for 34 times and incredible for 1 time, the success rate of the interaction was 97.14%.

Also, the reputation value of terminal M to terminal X which had a bad reputation fell to the complete mistrust area according to the simulation. In the simulation, terminal M thought terminal X as incredible for 35 times and do not interact with X. But there were 7 times, the reputation value of terminal X fell in the gray area and M decided to give X a chance and interacted with X. So the interaction rate to the terminal X which had a bad reputation was 16.67%.

In the simulation, terminal M interacted with other terminals for 364 times. And it would check 9 other terminals for reputation value before each interactions, therefore, it sent 3726 times of query in the simulation.

B. Importance Fuzzy Subsystem

Importance fuzzy subsystem was simulated in this part. Monetary value, the criticality of the result and the time needed, as the input of the subsystem, was randomly generated. Fig.4 and Fig.5 will show the similar result in no-fuzzy system. Even, the ratio of interactions which terminal M perform on terminals with good or bad reputation was similar. In which, as Fig.4 shows, the ratio of terminal M interacted with O which had a good reputation was 96.4%(27 times of the 28 times), interacted with disreputable terminal X for 28% (7 times of the 35 times), interacted with the disreputable terminal X and Y for 20%(16 times of the 80 times).

But, the bandwidth had been saved by introducing the concept of importance. In the simulation, terminal M attempted to other terminals for 367 times and merely checked reputation value for 1431 times. Thus, terminal would query about 4 terminals before each interaction. It indicated that about 56% of the bandwidth had been saved compared with no-fuzzy system by introducing the importance fuzzy subsystem.

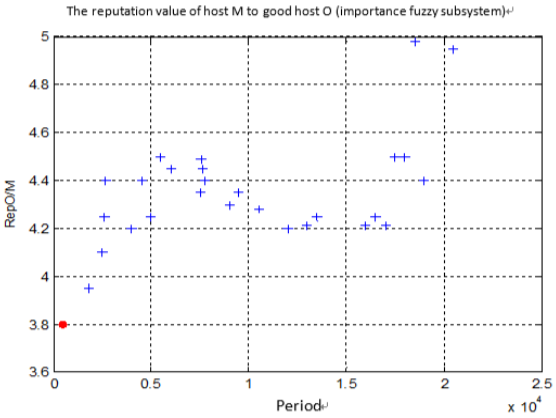

Figure 4. The reputation value changes of M to O after using the importance fuzzy subsystem.

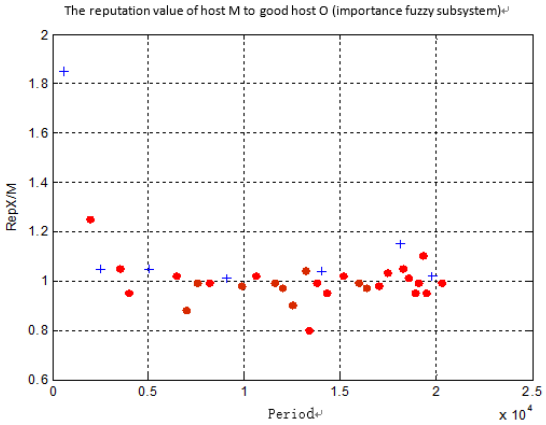

Figure 5. The reputation value changes of M to X after using the importance fuzzy subsystem.

C. FDecision Fuzzy System

The previous procedure would be repeated in this section, stimulating FDecision subsystem. For this part, we would divided the character of a terminal into gullible or paranoid: each terminal was given a gullible level from 0 to 10, 10 is the highest gullible level. For the other two inputs of FDecision subsystem, the importance value of each interaction was generated randomly, and the reputation value could be calculated according to formula (4). Also, the interactions between gullible terminal M,

paranoid terminal Q and terminals with good or bad reputation had been studied.

For the gullible terminal M, the value of $repO/M$ increased after each attempt of interaction and kept its stability in the complete trust area at last. Q interacted with O for 33 times among 33 times of interaction attempts. This is mainly because O was a reputable terminal and M is a gullible one. For disreputable terminal X, the value of $repX/M$ would decreased into the complete mistrust area. But M interacted with terminal X for 35.7% (15 times of the 42 times) and terminal X, Y for 27% (24 times of 87 times). Surely, the number of queries for reputation value of terminal M was similar as no-fuzzy subsystem.

For the paranoid terminal Q, the value of $repO/Q$ increased after each attempt of interaction and kept its stability in the complete trust area at last. As Fig. 6 shows, Q interacted with O for 36 times among the 36 times of interaction attempts. This is mainly because terminal O was reputable, although Q was paranoid, it would still consider Q as credible. The reputation value of O in the first attempt of interaction was about 2.85, but the importance was very low. So, even if the reputation value was somehow incredible the paranoid terminal Q still wanted to give O a chance. O was a reputable terminal and kept its reputation from the beginning to the end.

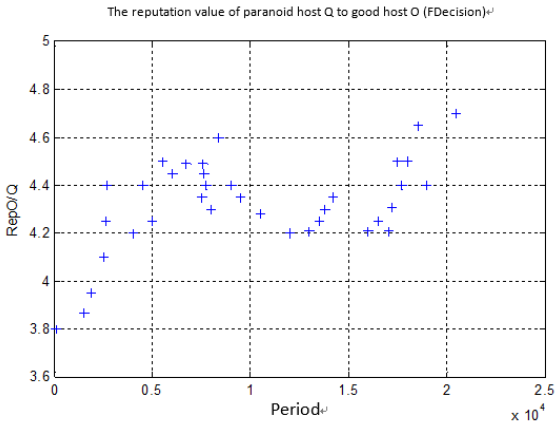

Figure 6. The change of reputation value of Q to O after using the FDecison fuzzy subsystem.

Fig. 7 shows the value of $repX/Q$ which Q had on bad terminal X. Because the importance of the transaction is very low, terminal Q only gave X a chance in the first attempt, and the value of $repX/Q$ in it was 2.2. Q didn't interact with X after that because the value of $repX/Q$ was always in the gray area. In the simulation, the rate of credibility of X from the view of Q was 2.6% (1 time of the 38 times), and the probability that bad terminal X and Y were both credible was merely 2.7% (twice in 71 times). This means, Q was hardly possible to interact with bad terminals in this model. The number of queries of reputation value was just similar as no-fuzzy system.

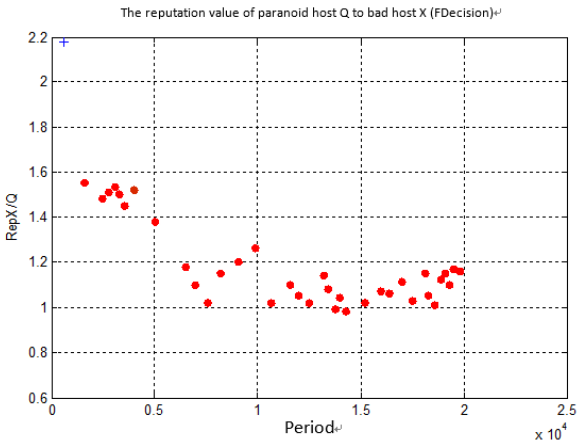

Figure 7. The change of reputation value of Q to X after using the FDecision fuzzy system

D. RI Fuzzy Subsystem

The role of RI fuzzy subsystem in the model is studied in this part. There are three inputs in the fuzzy subsystem: the accuracy of the result needs to be recalculated after each interaction, the time of an interaction (compared to expected time) and randomly generated monetary value.

The change of $repO/M$ is shown in Fig.8, although the value of $repO/M$ increased, the majority of it still fell in the gray area. So, RI subsystem introduced some new concepts under such condition. A good terminal O always had very nice interactions, but the accuracy of result, the input of the fuzzy subsystem was still need to be considered. The RI value of O would not bigger than 4 normally due to the other two randomly generated inputs of the subsystem. And, because terminal O did not have enough interaction times and importance, it wasn't thought as a reputable terminal. We shall see the reputation value of terminal O which had the right result also fell into the gray area shortly after. Terminal M only interacted with O for 80% (28 times of the 35 times). When it comes to bad terminal X, its reputation value decreased and fell into complete mistrust area. The outcome showed that the accuracy of the result weighted more higher in the RI subsystem. So, if the result of an interaction was not correct, the terminal could be considered as a bad terminal. As the simulation showed, terminal M considered X was only 21.3% credible (10 times of the 47 times) and X, Y combined was 22.3% credible (21 times of the 94 times).

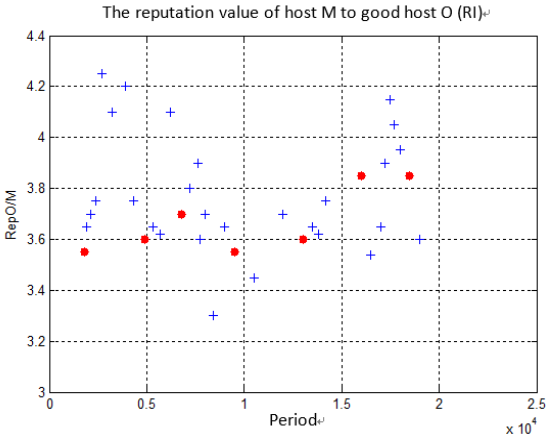

Figure 8. The reputation value change of M to O after using the RI fuzzy subsystem

In the simulation, the number of reputation vectors be queried was similar as the no-fuzzy system. Terminal M attempted to interact for 382 times, checked 9 terminals each time and sent 3438 request in all.

E. Comprehensive Simulation

We combined three fuzzy subsystem and simulated the whole system. Each terminal had certain degree of credibility. The inputs of Importance subsystem, monetary value, criticality of the result and time needed was generated randomly. The inputs of FDecision: gullible and paranoid were the character of a terminal, the importance came from the Importance subsystem, reputation value was calculated by the model. For RI subsystem, result (accuracy) was calculated after each interaction, time (about expected time) was randomly generated, and monetary value was the same as the value in the Importance subsystem. Additionally, TA=100, cooperation value Co=2, that was, terminals in the system would not query reputation vector for more than once within the 1000 cycles and would not check the terminals whose cooperation value smaller than 2. And terminal O was always set to be a good terminal while X was always a bad one.

The result of the simulation showed that, for gullible terminal M, the value of $repO/M$ increased and fell in the complete trust area. The rate of interactions between terminal M and O was 100% (28 times of the 28 times). The value of $repX/M$ decreased and fell into the complete mistrust area. The interaction rate between terminal M and X was merely 17.5% (7 times of the 40 times). Terminal M only queried the reputation vector for 91 times in the 354 times of interaction attempts which was only 1/4 of them.

As can be seen in Fig. 9, for paranoid terminal Q, $repO/Q$ increased and fell in the complete trust area after 5 times of interactions. The rate which terminal interacted with Q was 92% (44 times of the 48 times). Because of the bad reputation of X, $repX/Q$ decreased and fell into the complete mistrust area. The rate of the interactions between terminal Q and X was 2% (once of the 47 times), but in the only one interaction, $repX/Q$ was 2.5, the importance was low. The number of queries of reputation vectors by terminal Q was 77 times which was only 1/5 of 392 times which was the interaction attempts.

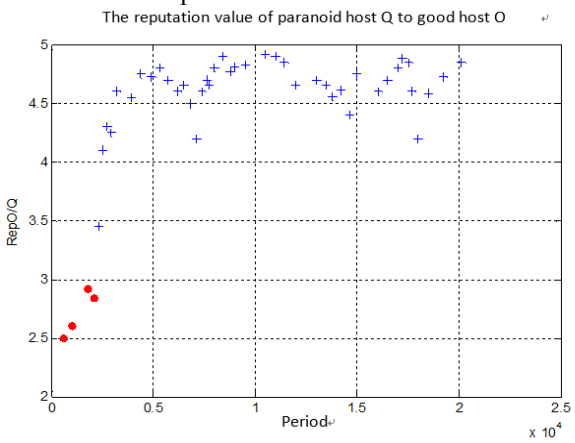

Figure 9. The reputation value change of Q to O in the comprehensive simulation

F. The Overhead and Security of the System

In this part, first, the network overhead of the CFMBRF system was assessed by evaluating the size of data of reputation information in network switching. Then we performed a stability test on checking the influence which the dishonest terminal had on the system through simulation.

In order to evaluate the system overhead, the experiment estimated the number of queries of reputation vectors, which could help in knowing the size of the data of reputation information switched in the network.

In the PATROL[6] system, each terminal needs to check other terminal before any interaction attempt. So every terminal needs to check 9 terminals before the interaction. But the number of terminals needed to be checked in CFMBRG was been limited according to the importance of the interaction through Importance subsystem. Because the three inputs of Importance subsystem was generated dynamically, the importance value and the number of terminals needed to be checked was distributed uniformly.

The simulation was performed according to different time interval TA. After that, assessing the number of terminals needed to be checked before each interaction attempt. As table 4 shows, when TA=0, each terminal would check about 4 terminals before attempt to interact. The number of terminals to be queried kept decreasing with the increasing of TA until every terminal could work independently without checking any reputation vector. The declining trend is in exponential shape, as is shown in Fig.10.

TABLE IV
THE INFLUENCE OF DIFFERENT TIME INTERVAL HAS ON THE NUMBER OF TERMINAL / THE NUMBER OF ATTEMPTS

TA	The number of terminals be checked	The number of attempts	Terminal number / attempt number
0	15616	3953	3.95
25	10508	3947	2.66
50	7896	3953	2
100	5204	3949	1.32
200	3154	3955	0.8
500	1445	3945	0.37
1000	782	3962	0.2
2000	389	3946	0.1
3000	272	3947	0.07
4000	210	3942	0.05
5000	153	3948	0.04

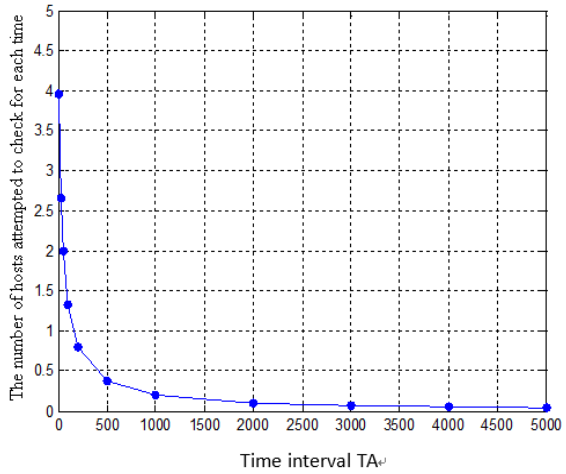

Figure 10. The picture of the tendency for the number of the checked hosts when TA increased.

As described previously, the reputation vector contains terminal identifier (IP address), reputation value, added together to 9 bites. Addition with the overhead of the head of the data, a reputation vector cost about 64 bites. Assuming that the importance of interaction in our system is random, therefore, each terminal needs to check 45% of other terminals on average and each terminal would want to check all the reputation values in every time interval TA in the worst condition. Table 5 shows the minimum TA permitted when the minimum bandwidth utilization were 100kbps and 1Mbps respectively. Table 6 shows the minimum TA permitted in the model without Importance subsystem when the minimum bandwidth utilization were 100kbps and 1Mbps respectively.

TABLE V
THE MINIMUM TA PERMITTED UNDER THE GIVEN BANDWIDTH UTILIZATION

The number of terminals	TA below the overhead of 100kbps	TA below the overhead of 1Mbps
10	0.21s	0.02s
20	0.88s	0.1s
50	5.6s	0.56s
100	22.8s	2.28s

TABLE 6
TA UNDER THE GIVEN BANDWIDTH OVERHEAD (NO IMPORTANCE SUBSYSTEM)

The number of terminals	TA below the overhead of 100kbps	TA below the overhead of 1Mbps
10	0.46s	0.05s
20	1.9s	0.2s
50	12.5s	1.3s
100	50.7s	5.1s

Comparing the two tables, it can be found that the system could still keep more new reputation information even TA became half of the original value with the Importance fuzzy subsystem under the condition that the network bandwidth was not influenced. But the change of TA was still under the influence of the importance of the interaction, if the importance of interaction was consistently in a high level, TA would be similar as table 6, but if the importance of interaction was consistently in a low level, TA would become lower even than table 5.

In order to check the stability of CFMBRF, that is, to check the critical number of dishonest nodes which CFMBRF could bear with and interact correctly, the simulating network (as Fig. 11 shows) which had 9 terminals and terminal Y which was always with a bad reputation would keep recalculating the value of $repY / M$ with the increase of dishonest nodes (which gave Y a very high reputation value) in the network. The value of $repY / M$ was still in the complete mistrust area and M could still sense that Y was bad in nature when the dishonest terminals in the system no bigger than 4. But when the dishonest terminals exceeded 4, $repY / M$ would exceed the normal value 2.5, even, when there were 7 or 8 dishonest terminals, $repY / M$ fell in the complete trust area.

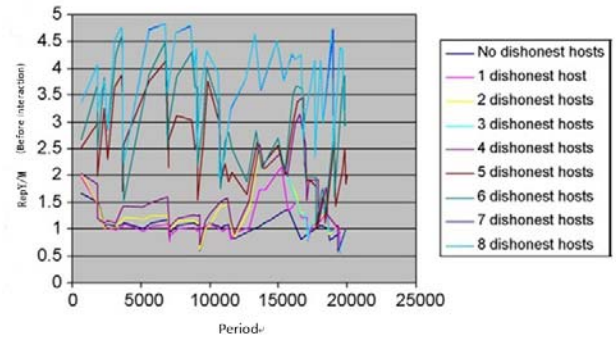

Figure 11. The change of RepY/M when the number of dishonest nodes is different

VI. CONCLUSION

This paper put forward a Comprehensive Trust Model based on Reputation and Fuzzy subsystems (CFMBRF) according to the method recommended. CFMBRF is an improved reputation-based trust model, taking into account the various important factors in reputation value calculation, such as, direct experience, reputation value, credibility of recommendation, dynamic decay factors based reputation value decay, the first impression and mixed recommendation by the terminals, and added with the subjective concepts such as "the character of terminal nodes", " importance of a interaction", "the decisions in the uncertainty region " and "setting the result of interaction" can be well used in the circumstances of Ubiquitous Network.

ACKNOWLEDGMENTS

This work has been funded by College Natural Science Foundation of Jiangsu Province (11KJB520002), Jiangsu 973 Scientific Project (BK2011023, BK2011022), the National Natural Science Foundation of China (61272419, 60903027), China postdoctoral Foundation (2012M521089), Jiangsu Postdoctoral Foundation(1201044C), Jiangsu Natural Science Foundation(BK2011370), Research Union Innovation Fund of Jiangsu Province (BY2012022).

REFERENCES

[1] Sabater J, Sierra C. Review on computational trust and reputation models[J]. Artificial Intelligence Review, Vol.24, No.1, pp. 33-60, 2005.

[2] Derbas G, Kayssi A, Artail H, et al. Trummar-a trust model for mobile agent systems based on reputation[C]//Pervasive Services, 200 ICPS 200 IEEE/ACS International Conference on. IEEE, pp. 113-120 2004.

[3] Ramchurn S D, Jennings N R, Sierra C, et al. Devising a trust model for multi-agent interactions using confidence and reputation[J]. Applied Artificial Intelligence, Vol.18, No.9-No10, pp. 833-852, 2004.

[4] Schlager C, Pernul G. Trust modelling in E-commerce through fuzzy cognitive maps[C], Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, pp. 344-351, 2008.

[5] Schmidt S, Chang E, Dillon T, et al. Fuzzy decision support for service selection in e-business environments[C], Computational Intelligence in Multicriteria Decision Making, IEEE Symposium on. IEEE, pp. 374-381, 2007.

[6] Schmidt S, Steele R, Dillon T S, et al. Fuzzy trust evaluation and credibility development in multi-agent systems[J]. Applied Soft Computing, Vol.7, No.2, pp. 492-505, 2007.

[7] Tajeddine A, Kayssi A, Chehab A, et al. PATROL: a comprehensive reputation-based trust model[J]. International Journal of Internet Technology and Secured Transactions, Vol.1, No.1, pp. 108-131, 2007.

[8] Xiong L, Liu L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. Knowledge and Data Engineering, IEEE Transactions on, Vol.16, No.7, pp. 843-857, 2004.

[9] Li Qianmu, Hou Jun, Qi Yong.A classification matching and conflict resolution method on meteorological disaster monitoring information [J]. Disaster Advances, Vol.6, No.1, pp. 415-421, 2013.

[10] Li Qianmu, Zhang Hong. Information Security Risk Assessment Technology of Cyberspace: a Review [J]. Information- an International Interdisciplinary Journal.Vol.15, No.11, pp. 4677-4684, 2012.

[11] Li Qianmu. Mulitiple QoS Constraints Finding Paths Algorithm in TMN [J]. Information- an International Interdisciplinary Journal.Vol.14, No.3, pp. 731-738, 2012.

[12] Qianmu Li, Jun Hou, Yong Qi, Hong Zhang. The Rule Engineer Model on the high-speed processing of Disaster Warning Information. Disaster Advances. Vol.5, No.4, pp. 432-437, 2012.

[13] Li Qianmu, Li Jia. Rough Outlier Detection Based Security Risk Analysis Methodology. China Communications. Vol.5, No.7, pp. 14-21, 2012.

Xianghe Wei, associate professor, the main research field is information security.

Hong Zhang, professor, Ph.D. supervisor, the main research fields are information security, data mining.

Xuan Mo, postgraduate student, the main research field is information security.

Yong Qi, professor, Ph.D. the main research field is sensor network node location.

Zhen Liu, postgraduate student, the main research field is information security.

Qianmu Li, professor, Ph.D. supervisor, the main research fields are information security and network performance diagnosis.