Ad-hoc multi-dimensional trust evaluation model based on classification of service

Li Yu, Cong Qian, Zuhao Liu, Ke Wang, Bin Dai

Department of Information Engineering, Huazhong University of Science and Technology, PRC,
Wuhan National Laboratory for Optoelectronics, Wuhan, Hubei, PRC
Email: hustqiancong@gmail.com

***Abstract*—Trust models studied before evaluated trust degree by the previous interactions of entities in ad hoc networks within a protocol. However, this way is not accurate and difficult to decide the trust value. The basic difficulty lies in the fact that trust information is often fuzzy and incomplete in an open network environment. The performance of mobile ad hoc network also is constrained by residual energy, delay, delay jitter and other factors. Thus a novel trust model with multiple decision factors is proposed, in which multiple decision factors, involving security trust and quality trust, are incorporated to evaluate trust. AHP (Analytic Hierarchy Process) methodology is used to combine these different factors in our paper. The requirements of the quality and security of nodes differ as services are different, so we also take the classification of service into consideration. Theoretical as well as simulation results show that our scheme is more accurate than the model evaluated just by the previous interactions of entities.**

I. Introduction

An ad hoc network is a kind of distributed system which lacks of strict centralized controls and its network topologies are rapidly-changing. All nodes are dynamic and arbitrarily located, and they are both users and providers of resource, equally, in Ad Hoc networks. Nodes have to cooperate with each other to support the network functions due to the lack of intermediate servers. Owing to this characteristic, the cooperation between nodes is very fragile. Therefore, a method called trust management frameworks is put forward. Trust schemes [1,6] or reputation system [2] has been proposed to evaluate the behaviors of nodes. The trust-based routing framework [3] put forward by Cheng Weifang etc can help to detect both unavailability of failed nodes and selective forwarding attacks of compromised nodes. The trust model in this framework only uses packet re-transmitting ratio and packet forwarding cooperativity to evaluate nodes behavior.

However, trust evidence may be uncertain and incomplete because of the dynamic nature of ad hoc Networks [4]. These problems can bring along hidden dangers for ad hoc networks, such as limited energy, increased packet loss ratio, delay, delay jitter etc. We can get the conclusion that evaluating trust from one angle is not enough to decide on whether or not to trust a specific node is obvious. Thus we propose a novel trust model in which multiple decision factors, involving security trust and quality trust, are incorporated to evaluate trust. Hence, we need to combine these trusts to get an overall trust in this new trust model.

Multi-service support is an important motivation for our proposed trust model. Services are classified in the network. The demand for node performance, such as quality and security vary with different types of service, thus consideration of service type in reliability measurement is necessary. There are many methods for combining different factors like Bayesian [5],in this paper we use AHP (Analytic Hierarchy Process) to combine these trusts.

The rest of the paper is structured as follows. The trust management is presented in section II, In section III, we describe some definitions and formulas about each trust. Section IV presents the approach, proposes Analytic Hierarchy process to combine these trusts. Section V provide theoretical and simulation-based analysis. Conclusions and areas of future research are given in Section VI.

II. Trust Management

The distrust node is a major potential security and quality risk for ad hoc network. According to the difference of target node, trust management system has divided distrust node into malicious node, selfish node, and low competitiveness node [6]. The acts of the above mentioned three types of distrust node always impact on security trust (transmitting, residual energy) or quality trust (delay ,delay jitter) directly. So we define this trust management to evaluate the performance of nodes, as shown in Fig. 1.

III. Definitions and Formulas

A. Transmitting trust

In this paper, transmitting trust means the relationship value calculated between two cooperation nodes in an ad hoc network which can send (receive) information to (from) each other. For a node of ad hoc network, packet lose ratio [7] is a very important factor to evaluate the behavior and the reliability of its neighboring nodes. Several ways of calculating the trust value have been proposed. In this paper, we calculate the transmitting trust using a Bayesian approach [8] based on beta distribution as the theoretic fundamental. This approach chooses two important parameters, trust value and confidence value, to describe the transmitting trust for a node. Trust value corresponds to the subject's estimation of the object's trust,

CHINACOM 2010, August 25-27, Beijing, China

DOI 10.4108/chinacom.2010.37

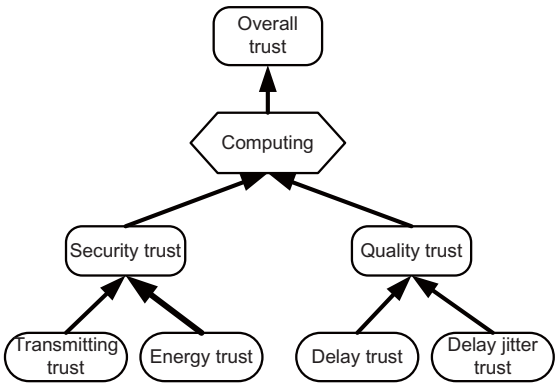

Fig. 1. A trust management in ad hoc network

while confidence value is an indispensable parameter that characterizes the statistical reliability of the computed trust. The trust value, t_k , associated with a node at time k is defined as the mean value $\mu(a_k, b_k)$ of the beta (a_k, b_k) distribution [9]:

$$t_k = \mu(a_k, b_k) = \frac{a_k}{a_k + b_k} \tag{1}$$

where $0 \leq t_k \leq 1$, a_k is the total number of successful interactions and b_k is the total number of unsuccessful interactions between two of nodes during a time. And the confidence value, c_k, associated with the trust value is defined to be a value related to the standard deviation of beta (a_k, b_k):

$$c_k = 1 - \sqrt{12}\sigma(a_k, b_k) = 1 - \sqrt{\frac{12 a_k b_k}{(a_k + b_k)^2 (a_k + b_k + 1)}} \tag{2}$$

,$0 \leq c_k \leq 1$.

If i is the subject node, j is the object node, and k is a group of neighboring node of i, then the trust value of i about j is,

$$T_{ij} = \frac{\sum_k t_{kj} \cdot c_{ik}}{\sum_k c_{ik}} \tag{3}$$

and the final confidence value of i about j is,

$$C_{ij} = \frac{\sum_k c_{kj} \cdot c_{ik}}{\sum_k c_{ik}} \tag{4}$$

B. Energy trust

Energy efficiency is one of the most important design constraints in ad hoc network architectures [10]. The lifetime of each node depends on its energy dissipation. Suppose that we don't consider about the residual energy, most nodes would choose the high 'trust' nodes to forward packets Frequently. However, in ad hoc networks, all nodes are energy-constrained and the lifetime of each node depends on its energy dissipation. This behavior will quickly drain the battery of these nodes and reduce the survival period of ad hoc networks sharply. In this paper, we combine the energy trust into the overall trust to balance the energy consumption of individual nodes, thus can enhance the security of networks.

In ad hoc networks, communication is usually the main source of energy consumption. The energy model [11] introduced by W.R.Heinzelman etc is used to evaluate the residual energy of the node according to the communication. In this model, if node sends n bit data to another node , then the calculating formula of the energy expended model for this node is defined as the following equation:

$$E_i(n) = n \cdot E_{elec} + E_{amp} \cdot d^2 \tag{5}$$

where E_{elec} is the energy per bit consumed by the transmitter electronics, E_{amp} is the energy consumed by transmit amplifier to achieve an acceptable signal-to-noise ratio (SNR) and d is the distance from node i to node j. E_{elec} and E_{amp} are given. In ad hoc networks, every node can only communicate with its neighboring nodes which are in its communication range. So d is equal to the communication range of nodes.

For node j, the energy consumed is:

$$E_j(n) = n \cdot E_{elec} \tag{6}$$

Moreover, nodes are also in charge of forwarding data packets of other nodes. In this process, nodes must be able to receive those packets and then forward data, the energy consumed is:

$$E_k(n) = 2 \cdot n \cdot E_{elec} + n \cdot E_{amp} \cdot d^2 \tag{7}$$

Based on this model, we can get the residual energy of every node in the network, and then compute the energy trust value.

The residual energy is:

$$ER_c = ER - E \tag{8}$$

where E is the energy consumed of one node, ER_c is the current residual energy of this node and ER is the previous residual energy of this node. If the node in the network has residual energy enough, it can perform normally. As the energy of this node is consumed, the residual energy becomes less and less. When it is reduced to a threshold E_d, the node would become ineffective.

According to this characteristic and the performance of nodes in the simulation, we can assume that energy trust and residual energy can meet the exponential relationship, as shown in fig. 2.

C. Delay trust

Delay is defined as the time that packets from the source to the destination. End to End delay is the sum of delays experienced at each hop on the way to the destination. In current networking, delay is an important measure of quality of service particularly for the high traffic such as voice or video traffic. The main objective of defining this trust is to address the question of how to estimate the impact of every node to the delay time. The delay time is:

$$DT_{ij}(n) = s_i - r_i \tag{9}$$

where s_i is the time of sending out by source node , r_i is the time of receiving by destination node j, DT_{ij} is the delay

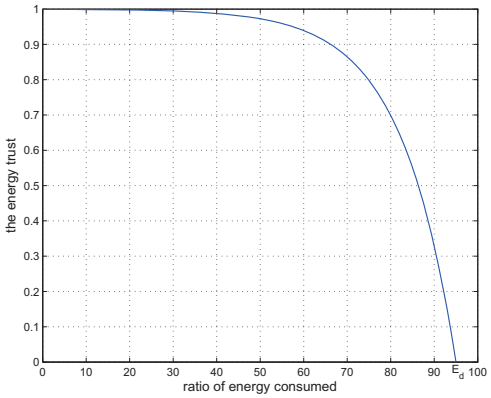

Fig. 2. The relationship between energy trust and residual energy of node in ad hoc network

time of packet n from node i to node j. If packet n is lost, r_j is undefined and $DT_{ij} = 0$.

The state of every node is changed as time changes. However, it is easy to understand that the influence of recent result of measure is more important than the past. So the weight of an older measure is less than that of a recent measure. An adaptive forgetting scheme is introduced where the forgetting factor is adjusted in time to model this influence decreasing phenomenon. In this scheme, a forgetting factor is introduced. Consequently, it avoids the case that the status of node changes. The value of delay trust is determined by:

$$TD_{ij}(n) = 1-(1+\frac{\sum_{k=1}^{n} DT_{ij}(k)\beta^{t_c-t_j}}{n} - DT_{thre})^2, 0 \leq \beta \leq 1 \quad (10)$$

where $TD_{ij}(n)$ is the nth evaluated delay trust of node i to node j, DT_{thre} is the threshold which can meet the requirements of the worst quality of service, β is the forgetting factor, t_c and t_j are the recent time and the past time respectively.

D. Delay jitter trust

In today's networking, when voice or video packets are transmitted over the ad hoc networks, packets may experience variable delay, called delay jitter. For non-real-time data transfer applications, such as ftp and telnet, delay jitter has little real impact on quality of service. By contrast, real-time data transfer applications such as audio, video and voice must be transmitted continuously. For this reason, the delay jitter trust is used to evaluate the performance of end to end delay jitter. Some cases are the reason, when there is a big delay jitter from node i to node j. Every reason should be taken into consideration. Firstly, the competence of node j is limited and is not able to satisfy the requiring quality of the service. Secondly, supposing node j is perfect that it could deal with any service. However, it may lead to this situation that excessive traffic flows go through this routing because they find this routing is good to complete their transmission. Thus it makes this routing become too crowded. so delay jitter trust is introduced to prevent these situations.

Delay jitter is defined as the variation between the delay of current packet and the average delay of packets before, then delay jitter can given by:

$$DJ_{ij}(n) = DT_{ij}(n) - \frac{\sum_{k=1}^{n} DT_{ij}(k)}{n} \quad (11)$$

The delay jitter trust defined as follows is similar with the delay trust:

$$TJ_{ij}(n) = 1-(1+\frac{\sum_{k=1}^{n} DJ_{ij}(k)\beta^{t_c-t_j}}{n} - DJ_{thre})^2, 0 \leq \beta \leq 1 \quad (12)$$

where $TJ_{ij}(n)$ is the nth evaluated delay trust of node i to node j, DJ_{thre} is the threshold which can meet the requirements of the worst quality of service, β is the forgetting factor.

IV. Combining Trust Using AHP Methodology

In our trust model, building an overall trust depends on four aspects which are transmitting trust, energy trust, delay trust, and delay jitter trust respectively. Obviously, voice and video services often have more restrictive quality requirement on delay and delay jitter than data transfer services such as web browsing have. So the weighting coefficients are given in accordance with the service differentiation. AHP (Analytic Hierarchy Process) methodology is used to calculate the overall trust in our paper.

AHP, a method [12] which converts semi-qualitative and semi-quantitative problems into quantitative issues, was put forward by American Professor T.L.Saaty in mid-1970s and revised in 1994.The basic idea that is to find out the involved main factors, then constituted a hierarchy model, according to association affiliation of the factors. After that defining the relative importance of each factor by comparison of factors and then makes a comprehensive judgment. The advantage of AHP method combing with qualitative analysis and quantitative analysis, which aims to reduce the disadvantage brought by subjective assume and make evaluation more reliable, is that the judgment will be quantified expressed and dealt with. AHP is mainly used in multi-objective decision making. On this account, AHP is utilized for combining the trusts of different aspects for different services.

The computation of AHP involves several steps as follows:

Step1: Establish the "trust hierarch" for evaluating complex problems.

The trust hierarch must include:

1. The overall trust
2. The factors that must be weighted
3. The alternative choices

Step2: Establish pair-wise comparisons of all alternatives.

After establishing hierarchy structure, construct pair-wise comparison matrix by compare the importance of judgments in the same level. Each factor must be compared with all other factors. This process is accomplished using a weighting

table that ranges in values from 1 to 9, which shows in table 1.

Table 1. The fundamental scale

Scale	Meaning(factor i compared by factor j)
1	Equal Importance
3	Moderate Importance
5	strong Importance
7	Demonstrated Importance
9	Extreme importance
2, 4, 6, 8	Medium value among comparison referred above
1.1∼1.9	If the importance are very close

Suppose that there are n factors, then we can obtain a comparison matrix $\mathbf{A} = (a_{ij})_{n\times n}$

Step3: Sort these factors on the same level and test consistency.

By using the previous comparison matrix $\mathbf{A}$, compute a set of weighting vector first and then carry out consistency test to this weighting vector for avoiding a wrong estimating.

The process is listed as follows:

Normalize each column of the matrix $\mathbf{A}$.

$$\overline{w}_{ij} = a_{ij} / \sum_{i=1}^{n} a_{ij} (j = 1, 2, ..., n) \tag{13}$$

Get $\overline{w}_i$ through summing the $\overline{w}_{ij}$ by row, and then normalize $\overline{w}_i$.

$$\overline{w}_i = \sum_{j=1}^{n} \overline{w}_{ij} (i = 1, 2, ..., n) \tag{14}$$

$$w_i = \overline{w}_i / \sum_{i=1}^{n} \overline{w}_i \tag{15}$$

and $\mathbf{w} = (w_1, w_2, ..., w_n)^T$ Compute the largest eigenvector of matrix $\mathbf{A}$.

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^{n} \frac{\mathbf{A} \cdot \mathbf{w}}{w_i} \tag{16}$$

Calculate the indicators of matrix consistency and examine consistency. Here consistence index CI is adopted to examine the consistency, and defines $CI = (\lambda_{max} - n)/(n-1)$. The smaller the value of CI is, the higher degree of consistency of matrix $\mathbf{A}$ is. In order to determine the permissible range of non-consistency, Saaty introduced RI which means random consistence index. For different factor n, saaty obtain the RI, which shows in table 2.

Table 2. Random consistence index.

n	2	3	4	5	6
RI	0.00	0.58	0.90	1.12	1.24
n	7	8	9	10	11
RI	1.32	1.41	1.45	1.49	1.51

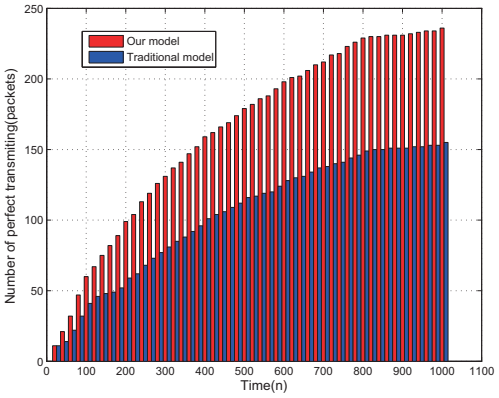

Fig. 3. The comparison of our model and the traditional model when there are 30% bad nodes

$$CR = \frac{CI}{RI} \tag{17}$$

where CR is called as rand consistence rate. When $CR < 0.1$ or around 0.1, the matrix $\mathbf{A}$ is satisfying consistency. Otherwise, we should revise the matrix $\mathbf{A}$.

Step4: Sort and test consistency in the whole system. The sequence of higher level is synthesized by the results of single sorting.

After these 4 steps, four aspects of trust can be combined into the overall trust according to the corresponding weighting vector.In this section, we know how to establish the overall trust assessment, and this scheme is used in next section.

V. Simulation Results and Analysis

Our model was implemented and evaluated in Matlab. Two simulation scenarios are presented. During our simulations, a flat, rectangular area of $100m \times 100m$ is the whole environment where 100 nodes are deployed and fixed randomly in this area. The physical layer uses a fixed transmission range model, where two nodes can directly communicate with each other only if they are within certain transmission range. We set the transmission range to $7m$. At initial time $(t = 0)$ of this system, trust values of transmitting, energy, delay and delay jitter are set to the maximum value 1 uniformly and the residual energy rate of every node is set to 1.

In the first simulation scenario, the fixed rate of nodes which perform badly in different aspect (long time delay, high packet loss ratio etc) was adopted, and then the different proportion of these nodes will be discussed. Every node has the same overall trust value, and the source nodes randomly select a node as destination node for data packets forwarding at the beginning. After several numbers of transactions, the reliable nodes can get higher trust value and some nodes whose performance of certain aspect such as security or quality is poor can only get lower trust value correspondingly. To study the performances of the presence of misbehavior in ad hoc networks, the metric of perfect transmitting ratio will be measured. The perfect

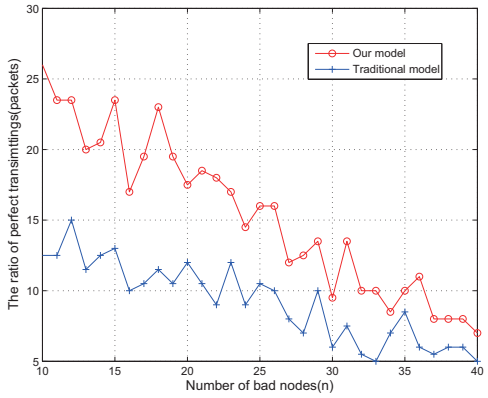

Fig. 4. Node Performance Comparison of the two models with the increasing of bad nodes

transmission is defined that all the nodes in the path must be meet the minimum requirements for the various property indexes at the moment rather than just transmitting the packets successfully. In this paper, four types of service are chosen for simulation. The minimum requirements for the different property indexes vary with classification of service. As shown in figure. 3, where x-axis is represented as the times of traffic flow, and y-axis is represented as the number of perfect transmission. We can get the conclusion from figure. 3, the system performance using our trust model is much better than the traditional one. It was found that our model can achieve more reliable trustworthiness than the traditional model. Although the simulation results show that there is only small increase in both models in the final phase, that is because mobile nodes will be powered by batteries with limited capacity. Power failure of a mobile node affects not only the node itself but also its ability to forward packets on behalf of other nodes. So in the final stage of simulation, the life time of the overall networks is becoming over.

In next simulation, different proportions of nodes in worse states are given. Fig. 4 shows that as the percentage of nodes which perform badly in some aspects increases from 10% to 40%, the ability of both models decrease, but traditional model decrease more. When the rate of these nodes in worse state comes to 40%, the number of perfect transmitting almost reduced to zero. This phenomenon is obvious, because the bad nodes will lead to the most failure of the transmission. However, we can find that our model performs better than the traditional one. It is proved that our model is robust.

VI. Conclusions

Providing security in ad hoc networks is a major requirement, however quality is also a very important index to decide the trust of nodes, especially for the multimedia traffic. Considering that the requirements for the quality or security of nodes vary with the types of services, this paper has proposed a multi-dimension trust model based on classification of services, which is motivated to measure the trust of nodes in a complex network environment, especially when the types of services change. Our approach enables each node in the networks to establish an overall trust which combines major property trusts. This scheme can adapt to the transformation of services, and no matter how the services change, it can obtain a relatively reliable overall trust value to determine the routings. Based on the classification of service, we utilize the method of AHP for combining trusts of major property and then obtain the overall trust. Through the trust value, the status of every node can be predicted.

Our simulation experiments demonstrate the effectiveness of multi-dimensional trust evaluation model based on classification of service about evaluating the trust of model. In ongoing work, we are studying how to extract some of parameters in the network to judge the types of service.

Acknowledgment

This work was supported in part by National 863 Projects of China (2009AA01Z205), Fund of National Laboratory (P080010), Funds of Distinguished Young Scientists (2009CDA150), International Cooperation Project (S2010GR0445), Natural Science Foundation of China (60972016,60872010), Natural Science Foundation of China under Grant No. 60803005 and Program for New Century Excellent Talents in University (NCET070339).

References

[1] A. A. Pirzada and C. Mcdonald, "Trust Establishment In pure Ad-Hoc Networks", *Wireless Personal Communications*, vol.37, no.1-2, pp.139-168, April 2006.

[2] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks", *Proc. P2PEcon*, Harvard Univ., Cambridge, MA, June 2004.

[3] Cheng Weifang, Liao Xiangke, Shen Changxiang, Li Shanshan, "A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks", *WASA*, pp.478-489, 2006.

[4] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks, *in Proc. ACM Workshop Wireless Security*, pp.1C10, Oct. 2004.

[5] Yao Wang and Julita Vassileva, "Bayesian Network-Based Trust Model", *in Proceedings of the IEEE/WIC International Conference on Web Intelligence*, pp.372-378, Oct. 2003.

[6] Yan (Lindsay) Sun, Zhu Han, and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks", *IEEE Communications Magazine*, vol.46, no.2, pp.112-119, February 2008.

[7] A.Perrig, R.Szewczyk, V.Wen, D. culler, J.Tygar, "SPINS:security protocols for sensor networks", *in Seventh Annual ACM International Conference on Mobile Computing and Networks(Mobicom 2001)*, Rme, Italy, July 2001, pp.189-199.

[8] Jian-Jun Qi, Zeng-Zhi Li an Ling Wei, "A trust model based on Bayesian approach", *Third International Atlantic Web Intelligence Conference*, pp. 374-379, 2005.

[9] Charikleia Zouridaki, brian L.Marek Hejmo and Roshan K. Thomas, "Hermes: A quantitative trust establishment framework for reliable data packet delivery in MANETs", *Journal of Computer Security*, vol.15, no.1, pp.3-38, 2007.

[10] P. Havinga and G. Smit, "Design techniques for low-power systems", *Journal of Systems Architecture*, vol 46, no.5, pp.1-21, 2000.

[11] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. "Energy efficient communication protocol for wireless microsensor networks". *In Proceedings of the IEEE Hawaii International Conference on System Sciences*, January 2000.

[12] Satty Thomas L. "How to Make a Decision: The Analytic Hierarchy Process". *European Journal of Operational Research*, vol. 48, no. 1, pp.9-26, Sept.1990.