2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications

A Novel Trust Management Mechanism for Mobile Ad hoc Networks Based on Grey Theory

Fang Zhifeng, Zhang Kun
Information Institute
Shandong University of Political Science and Law
JiNan, China
E-mail: jcjxsd@126.com

***Abstract*—Trust management mechanism is a hot spot in the research of mobile Ad hoc network security. In view of the many problems of trust management mechanism in mobile hoc Ad networks，combining with the characteristics of mobile Ad hoc network, we present a mobile Ad hoc network trust management mechanism based on grey theory in this paper and apply it to the mobile Ad hoc network management in order to improve the availability and effectiveness of trust management mechanism and safeguard the security of mobile Ad hoc networks.**

***Keywords*- trust management mechanism; Grey theory; mobile Ad hoc networks**

I. INTRODUCTION

With the rapid development of mobile communication technology, mobile Ad hoc network as an important form of wireless network comes into being. Mobile Ad hoc network is the consortium of the mobile nodes not depending on any fixed infrastructure. Due to no infrastructure support, highly dynamic, support mobile communications, etc., mobile Ad hoc networks have a wide range of applications in the field of military field, moving the meeting, disaster assistance, intelligent office environment. However, the routing mechanism technologies have a big difference between mobile Ad hoc networks and traditional wireless network. This also makes the mobile Ad hoc facing more serious security threats. So we need to study more complete security solution. Currently, the trust management is an important research field of mobile Ad hoc network security issues.

Trust management concept was first proposed by M.Blaze et al 1996[1]. It is to adopt a unified approach to describe and explain the security policy, security credentials and direct trust relationship authorization safety-critical operations. Trust management mechanism is introduced in the mobile Ad hoc networks and is used to judge the behavior of network nodes. This can effectively establish a trust relationship between nodes to build a reliable and trusted network environment. It is a new hot spot in recent years in mobile Ad hoc network routing protocol security problems research area. However, with further research, security problems of trust management mechanism itself attract more and more attention. Because of mobile Ad hoc network nodes inherent limitations, time and space costs to calculate and share trust values affects the life of the node itself greatly. On the other hand, due to the establishment of a trust relationship between nodes depends on the recommendation of the third nodes, false recommendations and non recommendation behaviors of bad nodes poses a serious challenge to the trust mechanism itself. It has greatly affected the availability and effectiveness of the trust management mechanism. This also becomes a problem that must be solved by the trust mechanism.

In the past, there have been some trust management models based on probability distribution, evidence theory, fuzzy mathematics, semi rings and entropy. But these models require a higher quality of data. Some require a large amount of data, and some require data to be subject to a certain probability distribution. We can't use these trust management models when the data is small or unable to get the data distribution.

Recently, some scholars have introduced the grey theory to the research of trust management mechanism.

978-1-4673-8315-8/15 $31.00 © 2015 IEEE
DOI 10.1109/BWCCA.2015.33

Fu Cai [2] et al adopt an improved grey analysis method. This method can deal with the experimental data with multiple attributes, and calculate the gray correlation degree. This gives an effective method for network risk assessment. But in this method, the weight vector of each index of gray correlation degree is fixed. So once the intruder has defined the weight of the index in the system, the malicious node can disguise itself as a normal node according to the need. Jie Li [3] [4] et al propos a new trust management mechanism based on fuzzy set and grey theory-OTMF (Trust Management Framework Objective). They use multiple parameters to calculate the trust value, and have achieved good results. However, this model can only choose the probability of information exchange among nodes successfully as the input parameters for the calculation of the trust value [5]. So the accuracy of the results is not high. From the contents described above, we can see that the current research on the mobile hoc Ad network trust management mechanism has made some progress, but there are still a lot of problems.

In this paper, we use the grey theory to improve the trust management mechanism of mobile hoc Ad networks, and design a new trust evaluation method based on grey clustering analysis theory.

II. ALGORITHM

Supposing that we evaluate the trust degree of m nodes, each node selects n indexes, and gets the following evaluation matrix.

$$A_{m\times n}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}, \qquad (1)$$

the element x_{ij} is the value of the index j of the node i.

$i=1,\cdots,m \;\; j=1,\cdots,n$.

A. Entropy Weight Method

When evaluating the trust degree of the nodes, the different indexes have different influence on the degree of trust. We use the entropy weight method to determine the weights of different indexes. Entropy weight method is an objective method to determine the weights according to the size of different index entropy. The magnitude of the entropy reflects the difference of the index sequence data. The greater the entropy, the greater the difference between the indicator data. In order to make a better distinction between each node, the index having large entropy should be given a large weight, and the index having small entropy should be given a small weight. The weights of all indicators are 1.

Calculation steps:

Step 1: Because of the different units of the index, we must carry out the non dimensional treatment of the data. When the value of the index j is not exactly the same, the bigger the better positive indicators become:

$$x'_{ij}=\frac{x_{ij}-\min\limits_{j} x_{ij}}{\max\limits_{j} x_{ij}-\min\limits_{j} x_{ij}} \qquad (2)$$

The smaller the better the negative indicators become:

$$x'_{ij}=\frac{\max\limits_{j} x_{ij}-x_{ij}}{\max\limits_{j} x_{ij}-\min\limits_{j} x_{ij}} \qquad (3)$$

Evaluation matrix A becomes:

$$A'_{m\times n}=\begin{pmatrix} x'_{11} & x'_{12} & \cdots & x'_{1n} \\ x'_{21} & x'_{22} & \cdots & x'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x'_{m1} & x'_{m2} & \cdots & x'_{mn} \end{pmatrix} \qquad (4)$$

Step 2: We calculate the proportion of element x'_{ij} in the column summation, and write it down to

$$g_{ij}=\frac{x'_{ij}}{\sum\limits_{i=1}^{m} x'_{ij}}. \qquad (5)$$

Step 3: Calculate the entropy for each column:

$$e_j=-\frac{1}{\ln(m)}\sum_{i=1}^{m} g_{ij}\ln(g_{ij}) \qquad (6)$$

Step 4: Normalization to get the index weights:

$$w_j=\frac{e_j}{\sum\limits_{j=1}^{n} e_j} \qquad (7)$$

B. TOPSIS

TOPSIS (Technique for Order Preference by Similarity to an Ideal Solution) is C.L.Hwang and K.Yoon proposed in 1981. It is a sorting method using the proximity between evaluation objects and ideal target. It is a common method in multi objective decision analysis. The method considers such a node that close to the positive ideal solution and far from the negative ideal solution with high trust degree. Calculation steps are as follows:

Step 1: Firstly, the positive and negative ideal solutions are determined by using this method:

Positive ideal solutions:

$$X^{+}=(\max_{i} x'_{i1},\max_{i} x'_{i2},\cdots,\max_{i} x'_{im}) \quad (8)$$

Negative ideal solutions:

$$X^{-}=(\min_{i} x'_{i1},\min_{i} x'_{i2},\cdots,\min_{i} x'_{im}) \quad (9)$$

Step 2: Respectively calculate non dimensional index vector of node i and weighted distance with positive and negative ideal solution:

$$d_i^{+}=\sqrt{\sum_{j=1}^{m} w_j(x'_{ij}-\max_{i} x'_{ij})^2} \quad (10)$$

$$d_i^{-}=\sqrt{\sum_{j=1}^{m} w_j(x'_{ij}-\min_{i} x'_{ij})^2} \quad (11)$$

Step 3: The basic trust degree of node I is defined as:

$$\alpha_i=\frac{d_i^{-}}{d_i^{+}+d_i^{-}},\ 0\le\alpha_i\le 1 \quad (12)$$

C. Grey Fixed Weight Clustering

Then use grey fixed weight clustering method to classify the nodes. According to the data and experience obtained, we can divide the nodes into three categories: not too credible, credible, and more credible. The steps of grey clustering are as follows:

Step 1: According to the evaluation, we divide the value into 3 grey clustering in the light of the indicator j of evaluation objects, and determine the center point $\lambda_1,\lambda_2,\lambda_3$ of grey clustering 1, 2 , 3.

Step 2: Extending the gray to different directions, we consider increasing grey clustering 0 and 4 and determine the center point λ_0,λ_4. So we get a new central point sequence $\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_4$. We connect the point $(\lambda_k,1)$ with $k-1$ and $k+1$ center point of small grey clustering $(\lambda_{k-1},0)$, $(\lambda_{k+},0)$ and get the triangle whitening weight function of the index j on the grey clustering k : $f_j^k(\bullet)$, $j=1,\cdots,n$, $k=1,2,3$. For the observed value x of index j ,

$$\text{by } f_j^k(x)=\begin{cases}0, x\notin[\lambda_{k-1},\lambda_{k+1}]\\ \dfrac{x-\lambda_{k-1}}{\lambda_k-\lambda_{k-1}}, x\in(\lambda_{k-1},\lambda_k],\\ \dfrac{\lambda_{k+1}-x}{\lambda_{k+1}-\lambda_k}, x\in(\lambda_k,\lambda_{k+1})\end{cases} \quad (13)$$

We can compute the membership degree $f_j^k(x)$ belong to grey clustering k .

Step 3: We calculate composite clustering coefficient of node i ($i=1,2,\cdots,m$) on grey clustering k . $f_j^k(x'_{ij})$ is the whitening weight function of index j and subclass k . w_j is the weight of index j in composite clustering.

Step 4: According to $\max_{1\le k\le 3}(\sigma_i^k)=\sigma_i^{k^*}$, we judge that object i belongs to gray clustering k^* .

Step 5: We turn the language sets of not too credible, credible, and more credible into interval numbers $I_1=(0,0.3)$, $I_2=(0.3,0.7)$, $I_3=(0.7,1)$. If node i belongs to k^* grey clusterings, we write the comprehensive trust of node i to $\theta_i=\alpha_i I_{k^*}=\left(\overline{\theta}_i,\underline{\theta}_i\right)$. So each node will correspond to a comprehensive degree of trust of interval number type, assume

that $\theta_1, \theta_2, \cdots, \theta_m$. Using the method of [1] to sort the interval number. So we determine the type of node i.

III. Simulation Analysis

The experiment scenario uses ns-3 to create a wireless simulating environment and uses using 802.11 standards to simulate 6 wireless nodes in mobile Ad hoc network. $node\ i(i = 0,1,2,3,4,5)$). Node 0 wants to get the trust value of node 1 based on trust opinions from node 0 and its neighboring nodes 2, 3, 4 & 5.The DSDV routing protocol is used in the experiment scenario. All the nodes are static. The parameters observed are: packet loss rate; received signal strength; delay; throughput; data rate. Initially all parameters have equal weight.

Using the above algorithm, we can calculate direct, recommendation and indirect trust values of $node\ i(i = 0,1,2,3,4,5)$.

In Figure 1, there are the trust values of node 1 from node 0, 2, 3, 4, 5, and the total values with 3 nodes(including direct, recommendation trust values) and 5 nodes(including direct, recommendation and indirect trust values), the average value T10-average of T10~T15.

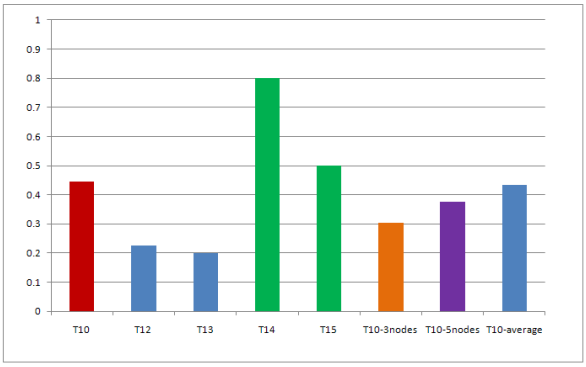

Figure 1 Trust values of node 1

From the figure, the results show that taking different relationship factors will affect the total value.

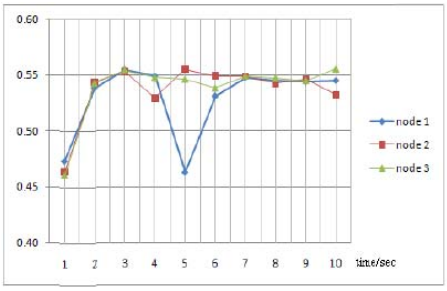

Figure 2 PLRs of node 1,2,3

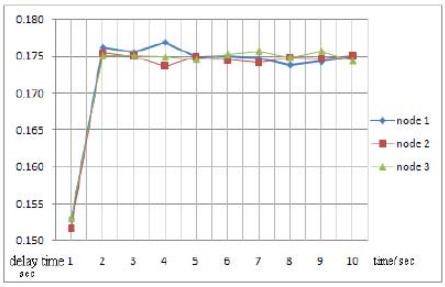

Figure 3 Delays of node 1,2,3

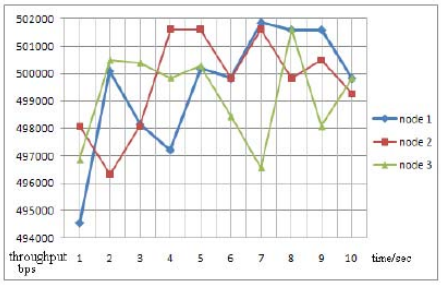

Figure 4 Throughput of node 1,2,3

Figure 2~figure 4 show that different parameters of different nodes will change significantly with time. So we should choose some more parameters to better reflect the state of the node.

Because there will be malicious nodes on some parameters, we should use several weight vector groups in order to obtain different trust values for a node; this can identify which aspect of a node's behavior is abnormal, compared with other neighbor nodes.

IV. Conclusions

In this paper, we present a mobile Ad hoc network trust management mechanism based on grey theory. First, consider choosing the indicators describing the nodes, such as packet loss rate, signal strength, data transmission rate, according to nodes' data by subjective and objective

method to determine the weight of each index. Then we construct a reasonable whitening weight function based on experience and data. Then the nodes are classified by weighted gray clustering method. Thus we can carry on the trust management to the nodes in the network. Simulation results show that it is an effective trust management mechanism. Further research will test the proposed trust management mechanism in more comprehensive environments in order to verify its validity.

V. ACKNOWLEDGEMENTS

We would like to thank anonymous reviewers for their invaluable comments on an earlier version of this manuscript. The authors are also grateful to the financial support provided by Shandong University of Political Science and Law research funding (No.2014Q01B& No.2014Z02B).

REFERENCES

[1] M. Blaze, J.Feigenbuam, J.Laey. "Decentralized trust management". Proceedings of the 17th Symposium on Security and Privacy. Okalnad,CA:IEEE ComPuterSoeietyPerss,164-173,1996.

[2] Fu Cai, Tang Fugui, Cui Yongquan, Liu Ming. "Grey Theory Based Nodes Risk Assessment in P2P Networks", 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications, 2009. 479-483.

[3] Jie Li, Ruidong Li, and Jien Kato. "Future Trust Management Framework for Mobile Ad Hoc Networks". IEEE Communications Magazine, vol. 46, no. 2, Apr. 2008. 108-114.

[4] Jochen Mundinger, Jean-Yves Le Boudec. "Analysis of a reputation system for Mobile Ad-Hoc Networks with liars". Performance Evaluation, Vol. 65, no. 3–4, March 2008, 212-226

[5] Nikos Dimitriou, Andreas Polydoros, Ahmed Barnawi. "Cooperative schemes for path establishment in mobile ad-hoc networks under shadow-fading". Ad Hoc Networks, Vol. 11, no. 8, November 2013. 2556-2566

[6]

[7] Forres S, Perelson AS, Allen L, Cherukun R. "Self-Nonself discrimination in a computer," Proc. Of the 94 IEEE Symp. on Research in Security and Privacy, Los Alamitos: IEEE Computer Society Press, 1994, pp. 120-128.

[8] Bykova M , Ostermann S , Tjaden B. "Detecting network intrusions via a statistical analysis of network packet characteristics," Proceedings of the 33rd Southeastern Symposium on System Theory. Ohio, At hens, 2001: 3092314.

[9] Hiren S,Jeffrey Ur,Anupam J. "Fuzzy Clustering for Intrusion Detection," The 12th IEEE International Conference on Fuzzy Systems, 2003, pp. 1274-1278.

[10] Hai J, Jianhua S, Hao Ch, Zongfen H. "A Fuzzy Data Mining Based Intrusion Detection Model," 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004:191-19.

[11] Kirkpatrick S, Gelatt C D, Vecchi M P. "Optimization by simulated annealing," Science, vol. 220, 1983, pp. 671-680.

[12] Portnoy L, Eskin E, Stolfo S J. "Intrusion detection with unlabeled data using clustering". In Proceedings of ACM CSS Workshop on Data Mining Applied to Security. Philadelphia, PA, 2001.

[13] LUO Min, WANG Li-na, ZHANG Huan-guo. "An Unsupervised Clustering-Based Intrusion Detection Method," Acta Electronica Sinica, vol. 31, 2003, pp.1713-1716.

[14] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.