AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Friend Based Trust Recommendation Model for Secure Quality of Service Aware Routing in Manet

[1]D.R. Jiji Mol and [2]S. Behin Sam

[1]Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore and Assistant Professor, Department of Computer Science, S.R.M Arts & Science College, Kattankulathur, Chennai
[2]Assistant Professor, Department of Computer Science, R.V.Government Arts College, Chengalpattu – 603 001.

Address For Correspondence:
S. Behin Sam, Assistant Professor, Department Of Computer Science, R.V.Government Arts College, Chengalpattu – 603 001.
E-mail: behinsam@gmail.com

ARTICLE INFO

Article history:
Received 12 February 2016
Accepted 18 March 2016
Available online 20 April 2016

Keywords:
QoS, MANET, Trust Recommendation, Trust Prediction, Collaborative Filtering

ABSTRACT

Background: A mobile ad-hoc network lacks a centralized control over its dynamic network topology thereby raising severe security issues while routing data packets from one node to another. Several protocols for secure routing have been proposed by various researchers. Recently more stress has been given on trust based models for secure routing. In these models trust computation plays a major role. Objective: In this paper we present a new method called Friend Based Trust Recommendation Model (FBTRM) for trust prediction of nodes which will help us in secure routing in ad hoc networks thereby increasing Quality of Service. Results: The results are generated by taking an example ad hoc network with twelve number of nodes. Conclusion: The method proposed in this paper uses collaborative filtering algorithm to predict the trust of a node using the trust values suggested by friendly nodes in the MANET.

INTRODUCTION

According to Mehran *et al*., (2004), the ad-hoc routing protocols are classified into three types, they are Pro-active (Table-driven), Reactive (On-demand) and Hybrid (Pro-Active/Reactive). The routing protocols have further been classified into three types by Siva *et al*., (2005) as Hierarchical, Geographical and Power aware. However, these classifications are not mutually exclusive as some protocols fall in more than one class. The operating environment of mobile ad-hoc networks is highly distributed that does not have a centralized authorization facility. Most of the existing protocols of the ad-hoc networks discover the paths between source-destination pair on the assumption that all nodes are legitimate and cooperating nodes. But in reality, according to Papadimitratos *et al*., (2002) a malicious node may enter the ad-hoc network and compromise the routing protocol functionality. Thus, the conventional routing algorithms are not sufficient to work efficiently in ad-hoc environment because of the presence of malicious node. Therefore collaboration and communication has to be made in a very cautious manner. Collaboration will be productive only if all the participants operate in a trustworthy manner. Hence, recently trust based secure routing protocols gained tremendous popularity. In this paper we have proposed a Friend Based Trust Recommendation Model (FBTRM) to find the trust of nodes in the network and these trust values can be used for routing data packets in a secure manner. This paper presents literature review of trust models and trust based routing protocols. The proposed friend based trust recommendation model is also discussed. The results and the discussion of the proposed model is also given followed by conclusion of the paper.

To Cite This Article: D.R. Jijimol and S. Behin Sam., Friend Based Trust Recommendation Model for Secure Quality of Service Aware Routing in Manet. ***Aust. J. Basic & Appl. Sci.,*** *10(8): 68-72, 2016*

Australian Journal of Basic and Applied Sciences, 10(8) April 2016, Pages: 68-72

Literature Survey:

Mobile ad hoc networks exhibit new vulnerabilities to malicious attacks or denial of cooperation due to their characteristics. Mobile nodes need to be equipped with efficient facilities to evaluate credibility values of other nodes.

Trust Models In MANET:

Trust' is one of the most complex concepts in social relationships, which is also an abstract psychological cognitive process, involving assumptions, expectations, behaviors, environments, and other factors. Similar to human society where one person trusts another to carry out an action, the concept of 'trust' can be introduced into MANETs to measure an expectation or uncertainty that an entity has about another's future behaviors. Most researchers are advocating the use of ratings and prefer making use of rating aggregation algorithms to evaluate the trust from several aspects (e.g., CPU usage, residual energy, bandwidth, etc.). However, these sophisticated models are not appropriate for MANETs where resources are limited and network topology is dynamic. Kannan Govindan *et al*., (2012) in his work presented a detailed survey on various trust computing approaches that are geared towards MANETs.

Liu *et al*., (2004) proposed a trust model for mobile ad hoc networks which uses both cryptography and trust. In this model, each node is initially assigned a trust level. The concepts discussed in this paper are generic and do not rely on centralized control, key distribution protocols, or any particular routing protocol. They can therefore be easily integrated into the current routing protocols used in mobile ad hoc networks. However, in the model, nodes may behave properly in order to gain a favorable status only to wait until a critical point in time where interrupting transmission might cause undesirable results.

In the model established by Sun Y.L *et al*., (2005,2006) trust is measured by entropy. They introduced an entropy function to represent the trust value between two nodes, which captured the dynamic nature of trust evidence. To compute the indirect trust value, Sun's models used trust value iteration techniques considering multi-level directed graph. When more nodes involved, the convergence speed of this method is exponentially slow, and its scalability becomes an issue.

Pirzada and McDonald (2006), presented a trust-based model for communication in pure mobile ad hoc networks that is based on individual experience rather than on a third party advocating trust levels. The model introduces the notion of belief and provides a dynamic measure of reliability and trustworthiness in this network. They also proposed an aggregation mechanism, where nodes calculate trust according to multiple observed events including acknowledgments, packet precision, gratuitous route replies, and blacklists.

With consideration of fuzzy set theory and reputation model, Luo and Fan (2010), proposed a subjective trust management model based on certainty-factor for MANETs (CFStrust), which can be used to quantify and evaluate the nodes' credibility. In their model, the problem of trust management is modeled by fuzzy likelihood estimation and confidence estimation. The trust evaluation mechanism emphasizes the contribution of direct interactions and the rationality of recommendation. However, it does not take a comprehensive account of the trust's attenuation problem, etc. This subjective trust model, in principle, can be applied to direct routing in MANETs.

Li *et al*., (2010), introduced a simple trust model based on packet forwarding ratio to evaluate neighbor's behaviors. In his model, a node trust is represented as a weighted sum of forwarding ratio of packets and a continued product of node trusts is computed as path trust. This evaluation provides a flexible and feasible approach to choose the shortest path from the candidates that meet the requirements of data packets for dependability or trust.

Hui Xia *et al*., (2013) presented a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes' historical behaviors, as well as the future behaviors via extended fuzzy logic rules prediction.

According to Antesar M. Shabat *et al*., (2015), the trust models that adopts recommendations by other nodes in the network faces challenging problems due to the risk of dishonest recommendations like bad-mouthing, ballot stiffing and collusion.

Friend Based Trust Recommendation Model (Fbtrm):

Methodology:

The proposed methodology to find the trust of a node is given in figure 1. This model uses the Find Friends module which in turn uses rate friends method proposed by Sanjay K. Dhurandher *et al*., (2011) to list out the friends of the source node. Once the list of friends in the network is ready, the model will seek Construct Matrix of Ratings module for trust recommendations from the friends identified in the previous module about all other nodes in the network. The obtained trust is stored in the Matrix of Ratings. Once it is ready we use Collaborative Filtering module to find the trust of the required node. The trust is stored in the trust table. This trust can further be used for routing data packets.

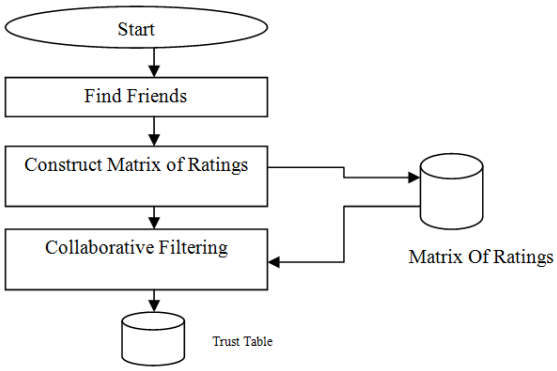

Fig. 1: Methodology To Find The Trust Of A Node

Let us consider an ad-hoc network which is newly initialized. Here each node is a stranger to another. The matrix of ratings given in Table 1 will be empty when the network is initialized.

Table 1: Matrix Of Ratings.

Node_ID	Node_Name	Node_Name
1	Trust_Value	Trust_Value
2	Trust_Value	Trust_Value
.	.	.
.	.	.

Find Friend method will find the friend node first and these friend nodes will uses trust values between numbers from 1 to 5. Nodes are encouraged to assign trust values based on how much they liked the behaviour of other nodes, with 5 highest and 1 lowest. Each node based on its personal experience, rewards collaborative nodes for their good behaviours and punishes them for their malicious actions. The trust values and their interpretations are given in Table 2.

Table 2: Trust Values of Nodes.

Trust_Value	Meaning
1	Poor Trust worthiness
2	Fair Trust worthiness
3	Average Trust worthiness
4	Good Trust worthiness
5	Excellent Trust worthiness

Once the Matrix of Ratings is ready at the source node, the proposed model uses Collaborative Filtering (CF) algorithm used in Paul Resnick *et al*., (1994) to predict the trust value of a node. The CF algorithm to predict the trust of node i by user *a* is denoted by $TP_{a,i}$ which uses a combination of trust ratings by the friends of user a that are already familiar with node i. The formula used for trust prediction is given as equation 1.

$$TP_{a,i} = \bar{r}_a + \frac{\sum_{u \in R} W_{a,u}(r_{u,i} - \bar{r}_u)}{\sum_{u \in R} |W_{a,u}|} \quad (1)$$

where $\bar{r}_a$ is the mean of ratings by *a* for other items, R be the set of users who have rated *i*, $r_{u,i}$ is the ratings of *i* by other users $u \in R$, $\bar{r}_u$ is the mean of ratings by user *u* and $W_{a,u}$is the correlation coefficient between user *a* and *u*. The above formula uses Pearson's correlation coefficient (PCC) by Pindyck. R.S., and D.L.Rubinfeld (1991) and Jonathan L. Herlocker *et al*., (2004) for calculating $W_{a,u}$.

RESULTS AND DISCUSSION

Let us take an example of a simple ad-hoc network containing 12 nodes which can be seen in Figure 2.

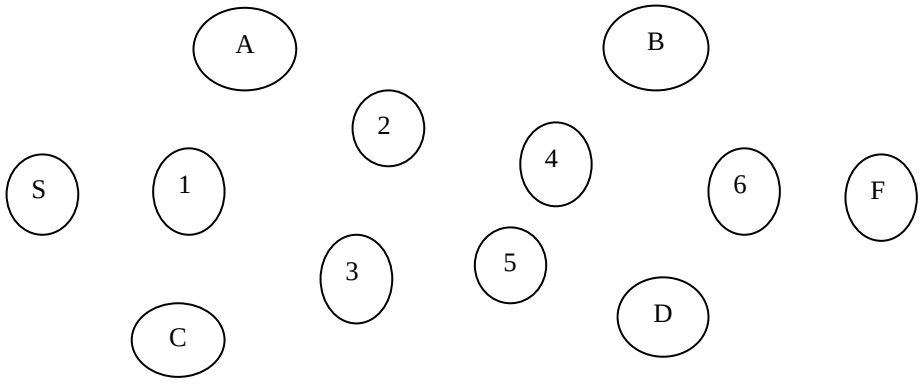

Fig. 2: Example Ad Hoc Network.

Let S be the source node and F be the destination node and A,B,C,D be friend nodes and they assign trust values to all the other nodes. The recommended trust values of these nodes are stored in the matrix of ratings given in Table 3.

Table 3: Recommended Trust Values Stored in Matrix of Ratings.

Node_Id	A	B	C	D
1	1	4	2	2
2	5	2	4	4
3			3	
4	2	5		5
5	4	1		1
6		2	5	

The proposed FBTRM uses the correlation coefficient(a value between -1 and +1) to tell how strongly two friend nodes are related together in assigning trust values to other nodes. A correlation coefficient of +1 indicates a perfect positive correlation. A correlation coefficient of -1 indicates a perfect negative correlation. A correlation coefficient near 0 indicates no correlation. The result shown in table 4 clearly shows that A and C are having perfect correlation. A and B has a negative correlation. A and D has no correlation. B and C has a negative correlation. B and D has a positive correlation. C and D has a perfect correlation.

Table 4: Correlation Coefficient Values.

	A	***B***	***C***	***D***
A	1			
B	-0.8	1		
C	1	-0.94491	1	
D	0	0.6	1	1

To predict the trust of any node use the formula given in equation 1. We have tried to predict the trust of node 6 by user A and the result was 4.56. This is a reasonable prediction for A, since the node received a high rating from a friend who agreed with him in the past and a low rating from a friend who disagreed.

Conclusions:

The goal of this paper is to present a trust computation method based on collaborative filtering algorithm which uses the trust recommendations received from the friends in the network. We have analyzed various literatures on trust computation and thus arrived at this new collaborative trust computational method for ad hoc network. The computed trust can be used by routing algorithm thereby increasing the quality of service of the ad hoc network.

REFERENCES

Antesar, M., Shabut, Keshav P. Dahal, Sanat Kumar Bista and Irfan U. Awan, 2015. Recommendation Based Trust Model with an Effective Defence Scheme for MANETs, IEEE Transactions on Mobile Computing, 14(10) : 2101-2115.

Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.M. Sha, 2013, Trust prediction and trust-based source routing in mobile ad hoc networks, Ad Hoc Networks, 11: 2096–2114

Jonathan, L., Herlocker, Joseph A. Konstan, Loren G. Terveen, John T. Riedl, 2004. Evaluating Collaborative Filtering Recommender Systems, *ACM Transaction on Information Systems* (TOIS), 22(1): 5–53.

Kannan Govindan, Prasant Mohapatra, 2012. Trust computation and trust dynamics in mobile adhoc networks: a survey, IEEE Communications Surveys & Tutorials, 14(2) : 279-298

Luo, J., M. Fan, 2010. A subjective trust management model based on certainty-factor for MANETs, Chinese Journal of Computer Research and Development, 47(3) : 515–523.

Li. X., Z. Jia, P. Zhang, R. Zhang, H. Wang, 2010. Trust-based on-demand multi path routing in mobile ad hoc networks', IET Special Issue on Multi-Agent & Distributed Information Security, 4(4): 212– 223.

Liu. Z., A.W. Joy, R.A. Thompson, 2004. A dynamic trust model for mobile ad hoc networks, In: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 80–85.

Paul Resnick, Neophytos Iacovou, Mitesh Suchak, Peter Bergstorm, John Riedl, 1994. Grouplens: An Open Architecture for Collaborative Filtering of Netnews, In: *Proc. ACM Conf. Computer Supported Cooperative Work*, ACM Press, 175–186.

Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz, 2004. A review of routing protocols for mobile ad-hoc networks, Ad-Hoc Networks, 2: 1-22.

Papadimitratos, P. and Z.J. Haas, 2002. Secure Routing for Mobile Ad Hoc Networks, In: Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 27-31.

Pindyck. R.S. and D.L. Rubinfeld, 1991. *Econometric Models and Economic Forecasts*. MacGraw-Hill, New York.

Pirzada A.A., C. McDonald, 2006. Trust establishment in pure ad-hoc networks, Wireless Personal Communications, 37(1): 39–168.

Sanjay, K., Dhurandher, Mohammad S. Obaidat, Karan Verma, Pushkar Gupta and Pravina Dhurandher, 2011. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems, IEEE SYSTEMS JOURNAL, 5(2): 176-188

Siva Ram Murthy, C. and B.S. Manoj, 2005. Ad-hoc wireless networks-architectures and protocols, Pearson Education Inc.

Sun, Y.L., Z. Han, W. Yu, K.J. Ray Liu, 2006. Attacks on trust valuation in distributed networks, In: Proceedings of the 40th Annual Conference on Information Sciences and Systems, 1461–1466.

Sun, Y.L., W. Yu, Z. Han, K.J. Ray Liu, 2005. Trust Modeling and Evaluation in Ad Hoc Networks, In: Proceedings of the Global Telecommunications, IEEE Computer Society Press.

Sun, Y.L., W. Yu, Z. Han, K.J. Ray Liu, 2006. Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE Journal on Selected Areas in Communications, 24(2): 305–319.