© 2017 IJSRSET | Volume 3 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Secured Path Evaluation Algorithm for Ad hoc Network

V. Asaithambi[1], Dr. N. Rama[2]

[1]Department of Computer Science, Govt. Arts College, Nandanam,Tamilnadu, India
[2]Department of Computer Science, Presidency College, Chennai,Tamilnadu, India

ABSTRACT

Mobile Ad hoc NETwork (MANET) is a wireless network with mobiles like nodes. The nodes in a MANET should be mutually trusted to each other and cooperate to each other. Then only the network can be said as a reliable network. The reliability of a MANET is depending on the reliability of each and every node in the network. The reliability of a node is evaluated in terms of trust value. In this paper the trust value of a node is calculated and the same is used for all other nodes in the network and also the total trust value of the network is evaluated. An intelligent algorithm is developed to secure the network using the trust value.

Keywords : RP, TT, DT, IT, IR, Black list.

I. INTRODUCTION

A Mobile ad-hoc network is a dynamic and auto-configuring wireless network. In which each and every node is a communicating device. Since this network is distributed everywhere, the devices are communicated directly each other. There is no specific topology is used in this network. So the attacks from malicious nodes are highly possible. The cause of the attacks may be from the outside of the network or from the inside of the network. The routed messages may be disturbed by the attacks from outside. The nodes become malicious to make an attack from inside. It is necessary to find the malicious nodes to protect the network.

This paper will give an idea to identify the malicious nodes in a network and by which the identified nodes can be ignored or removed from the network.

II. PROPOSED METHODS

Trust value model : The trust value model is shown in the following figure Fig.1. In which the information of a node is feed into the trust evaluation module. This trust table module categorize the nodes based on the threshold trust value and the trusted path is formed in trust path module. The malicious nodes are identified in the trust table module and the list is called black list. The nodes in the black list can be processed later depending on the measure of trust.

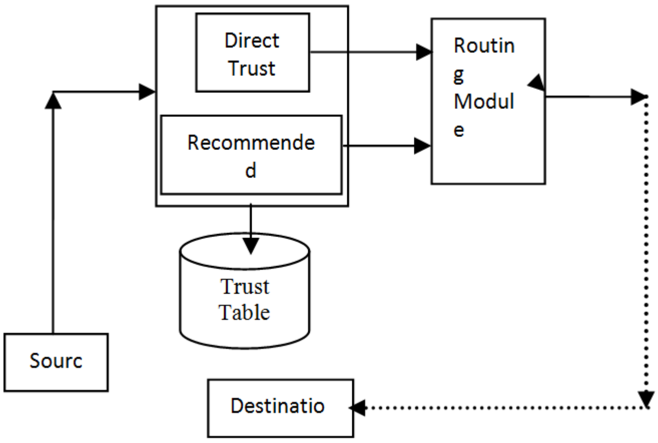

Figure 1. Trust Value Model

Trust Calculation : The previous interaction information of a node with other nodes are used to estimate the trust of a node. Depends upon the successful interactions the trust of a node becomes worthy. There are two types of trusts based on the nature of communication. They are direct trust and influenced trust. The direct trust is the trust between directly connected nodes. The influenced trust is the trust between two nodes with an influence of another node.

Direct trust calculation : Successful interactions between two neighbour nodes are considered after completing a set of interactions. Let a and b are any two nodes and SI(a,b) means successful interactions between a and b. It can be calculated as shown in equation(1).

$$DT_{a,b} = \sum_{k=1}^{n} SI_k(a,b) \tag{1}$$

Here $DT_{a,b}$ is direct trust by node a for node b. n is number of interactions between node a and node b. Similarly each node in the network is paired with every node in the network and the DT is calculated between each pair.

Influenced trust calculation: This is calculated by the measure of influence. For example, Let the interaction between two nodes a and b. Another node c is having previous experience with node b. This experience is shared with node a. Since the node b is influenced by node c, the node c influencing node a for node b. The measure of influence is influence for reliability(IR). It can be ignored when it is lesser than the given threshold trust (TT) value. The equation(2) gives the influenced trust of node b by node c for node a.

$$IT_{acb} = IR_{ac} \times DT_{cb} \tag{2}$$

Suppose the node a receives influence experience of node b from an influenced link L. Then the influenced trust is calculated using the following equation

$$IT_{aLb} = IR_{aL} \times DT_{db} \tag{3}$$

Where d is the destination node of the Link L.

If L=(a,1,2,3,4,...n,d,b) then use the following equation

$$IR_{ab} = DT_{a1} \times DT_{12} \times DT_{23} \times . . . \times DT_{nd} \times DT_{db} \tag{4}$$

Node a gives an objective estimate to all nodes in the link is as follows

$$IR_{aL} = \frac{\sum_{k=1}^{n} IR_{ak}}{n} \tag{5}$$

If there are d number of links as L_1,L_2,L_3, . . . ,L_d between node a and node b, node a gives an objective estimate of all influenced links.

$$IT_{aLb} = IR_{aL} \quad X \quad DT_{db} \tag{6}$$

Each link has weight W_L. Then the general weight W_{Lk} for the link L_k is calculated as follows

$$W_{Pk} = \frac{IR_{aPk}}{\sum_{k=1}^{n} IR_{aPk}} \tag{7}$$

Assuming that there are n links the influenced trust of node b can be calculated from node a is

$$IT_{ab} = \sum_{i=1}^{n} W_{Li} \quad X \quad IT_{aLib} \tag{8}$$

III. SAMPLE REPORTS

The following table will give the list malicious nodes, called blacklist. Based on the threshold trust (TT) the blacklist is generated.

Node	Trust value	blacklist
a	57	F
b	17	T
c	69	F
….		

Table 1 : Trust Table

IV. CONCLUSION

This paper will give an idea to identify the malicious nodes in a network based on the characteristics of the nodes. Threshold trust value is used like fuzzy logic. To improve the accuracy of the blacklist nodes, some other characteristics of the nodes can be used in future.

V. REFERENCES

[1]. C. J. Alpert and A. B. Kahng UCLA Computer Science Department, Los Angeles, CA 90024-1596 : A General Framework for Vertex Orderings, With Applications to Netlist Clustering

[2]. Danny Z. Chen, Ovidiu Daescu, Xiaobo (Sharon) Hu and Jinhui Xu Journal of Algorithms Volume 49, Issue 1 , October 2003, Pages 13-41 Finding an optimal path without growing the tree

[3]. Matti Nykänen and Esko Ukkonen, Department of Computer Science,University of Helsinki, P.O. Box 26, (Teollisuuskatu 23), 00014, Helsinki Finland Journal of

Algorithms Volume 42, Issue 1 , January 2002, Pages 41-53 The Exact Path Length Problem.

[4]. Daniel K. Blandford Guy E. Blelloch Ian A. Kash, Computer Science Department Carnegie Mellon University, Pittsburgh, PA 15213 fblandford,blelloch,iakg@cs.cmu.edu, An Experimental Analysis of a Compact Graph Representation.

[5]. www.cs.uni.edu/~schafer/courses/161/sessions/s09.ppt.

[6]. http://www.ugrad.cs.ubc.ca/~cs320/Lectures/cs320lec5.pdf.

[7]. http://www.personal.kent.edu/~rmuhamma/Algorithms/algorithm.html.

[8]. http://wwwin.cisco.com/cpress/cc/td/cpress/internl/dns/index.htm

[9]. Sabih H. Gerez.(1999) John Wiley & Sons, Algorithms for VLSI Design Automation.

[10]. N.A. Sherwani. (1999) Tata Mc Hill, Algorithm for VLSI Physical Design Automation.

[11]. Ellis Horowitz and Sartaj Sahni, (1999) Tata Mc Hill, Fundamentals of Computer Algorithms.

[12]. Matt Curtin (1997) Kent Information Services, Introduction to Network Security.

[13]. S. Anuradha, G.Raghu Ram, K.E.Sreenivasa murthy, V.Raghunath Reddy and D.R.Srinivas (2009) International Journal of Recent Trends in Engineering, DB Routing algorithm.