SECURE ADHOC ROUTING FOR DATA TRANSFER USING NEURO FUZZY

Suganya[#1] Nagarajan Srinivasan[*2]

[#]M.Tech, Advanced Computing, School of Computing, SASTRA University, Thanjavur, TamilNadu,India

[*]Assistant Professor, Department of computer science, SASTRA University, Thanjavur, Tamil Nadu, India.

[1]suganya.candy@gmail.com [2] nagarajan@cse.sastra.edu

ABSTRACT:-**In the present world the security vulnerabilities are highly challenging in MANET. To get the maximum security and minimum threat there is lots of work going on. To effectively isolate the malicious node this paper proposes a Neuro fuzzy algorithm. By using fuzzy logic we can further improve the security level by identifying the malicious node more accurately. The concept behind the paper is as in real life scenario, trust and sharing. Here in this paper we use the concept of trusting supporters, sharing the companion list and routing through data. In order to get a secure high trust level, fuzzy logic is applied for evaluating routing response and isolates the malicious node. Trusted route is evaluated in sequence of operation and data is transferred at a most trusted level. Trust values are computed to each node by setting verge values. The values of each node is checked with the verge value. If the value higher than the verge value mark it as high trusted node or else low trusted node.The fuzzy logic is implemented using aarmp routing protocol. Thus the level of trust is increased to obtain accuracy of identification. The goal of getting a robust route without any malicious node is achieved.**

Keywords- adhoc routing , Neuro fuzzy , MANET, security, AAMRP

I.INTRODUCTION

The wireless adhoc network is the network in which the wireless devices directly communicate with each other without central access point. [1] The nodes are randomly positioned in which each node acts as both host and router. Mobile adhoc network (MANET) is a kind of wireless adhoc network. In that routers are moving randomly and its topology may change rapidly.

MANET comprise of erratic host. It is not necessary that all the nodes in the network should be in the corresponding communication range. [2] Consider that two wireless hosts are not within the transmission range in ad hoc networks, other set of mobile hosts which is reside between them can lead their messages, so that complete network is formed within the mobile hosts.

The source node [3] can send the data packets through neighbour nodes to the destination node. The packet delivery is not granted if the neighbour node is a malicious node. Many methods are proposed to find out the malicious node but they are not accurately finding out the malicious node.

This paper proposes the neurofuzzy to accurately find out the malicious node using aarmp protocol [10]. Consider the neighbour node as a friend .Each node calculates the trust value of the friend node. If the trust value reaches the verge value then it is a trusty node otherwise it is considered to be the untrusted node. The data packets are sent through the trusty nodes.

II. RELATED WORK

In [1] ImrichChlamtac et al, proposed the directions and challenges of mobile adhoc networking. Important roles to take over in the future evolution technologies is carried out. The capabilities, applications and design requirements of mobile adhoc networking is described. In [2] Sung-Jib Yim et al,proposed that malicious nodes are detected using confidence level evaluation. All nodes keep its own and its neighbour confidence level. The confidence level is used to compute trustworthiness. Two parameters are used to distinguish malicious nodes from the normal nodes. By using this method malicious nodes can be accurately detected.In [3] Sanjay K. Dhurandher et al, proposed an algorithm to organize gaurded routing in mobile ad hoc networks. The authentication of nodes is done through challenges and friends concept. By using challenges, the information about the misbehaving node can be gathered vigorously. The rating of each node is calculated based on the packet it sent successfully. In [4] Idris M. Atakli, Hongbing Hu et al, proposed the weighted trust evaluation scheme is used to recognize the misbehaving node by monitoring its reported data. The Forwarded node provides the expectation value for each node. The expectation value of the particular node decreases when the node sends the meaningless information. In [5] Sanjay k. Dhurandher et al proposed a trust assignment and updating strategy to identify and to isolate the malicious node. T_req parameter is used to find the importance of content and type of the message. The path with high trust level can be used for message forwarding.

In [6] Jing-Wei Huang et al proposed the Message security in MANETS using a trust based multipath AOMDV combined with soft encryption. This scheme produces the minimum route selection time by deciding the message and path degree of secrecy. The trust mechanism conduces the idea of detecting malicious node by monitoring the packets. The trust value of the node changes according to the transfer time of the packets. In [7] Rangarajan A. et al proposed a multipath approach to message security in adhoc networks. Here data to be transmitted is split into many packets. Using jigsaw puzzle the split packets are combined together and sent using multipath routing. The tools used are multipath routing, all or nothing transforms and properties of polynomial. In [8] S. Nithya et al , proposed an Ant colony optimization technique to find the solution for computer problems. By this technique the best path can be found out from the available paths. Ant concept can be implemented using fuzzy logic. It is based on the amount of truth.

In [9] H. Hallani et al, proposed the trust level in a quantifiable manner between the sensor nodes in the adhoc network. The trust path is determined by the degree of trust value and the establishment. [10] Suparna Biswas et al, proposed that the nodes are randomly positioned in the network and transmission of packets without any guidelines of centralized node . Based on the trust value cluster head is chosen so that it will not be a malicious node.[11] Wei Gong et al, proposed that the expectation criterion of each nodes about its neighbours is observed through their neighbours.[12] Marjan Kuchaki Rafsanjani et al, proposed that the detection of unauthorized nodes, misbehaving nodes and the competence of the battery are computed. In order to prove their similarities ,there is no need of interchanging various messages.

III. MATERIALS AND METHODS

III. A..Experimental Setup

Ns2 simulator is used in the Redhat operating system. Because, we mainly focus on the immobility of the channel and route existence. The mobile noes are occurring in the area of 1500 X 800 m^2.The average hop length of a route is increased using square area comparably with smaller nodes. The transmission range is set to 250 units. The activity of the node is set to 10 m/Sec which is the maximum speed. The nodes are dynamic and the simulation time is about 500 Sec. The nodes involved in the simulation vary from 50 to 100.

The major part involved in this mechanism is that every node itself recognizes the malicious nodes accurately. The verge value is considered at each node. The choice of selecting the verge value plays a main role in finding the attacks in MANETS. When the drop rate of the packet is higher than the verge value, then the node is marked as malicious node.

The malicious nodes are finding out based on some verge values. After getting the appropriate node with certain trust values identify the nodes which are nearer to the destination node and then performs the transmission.

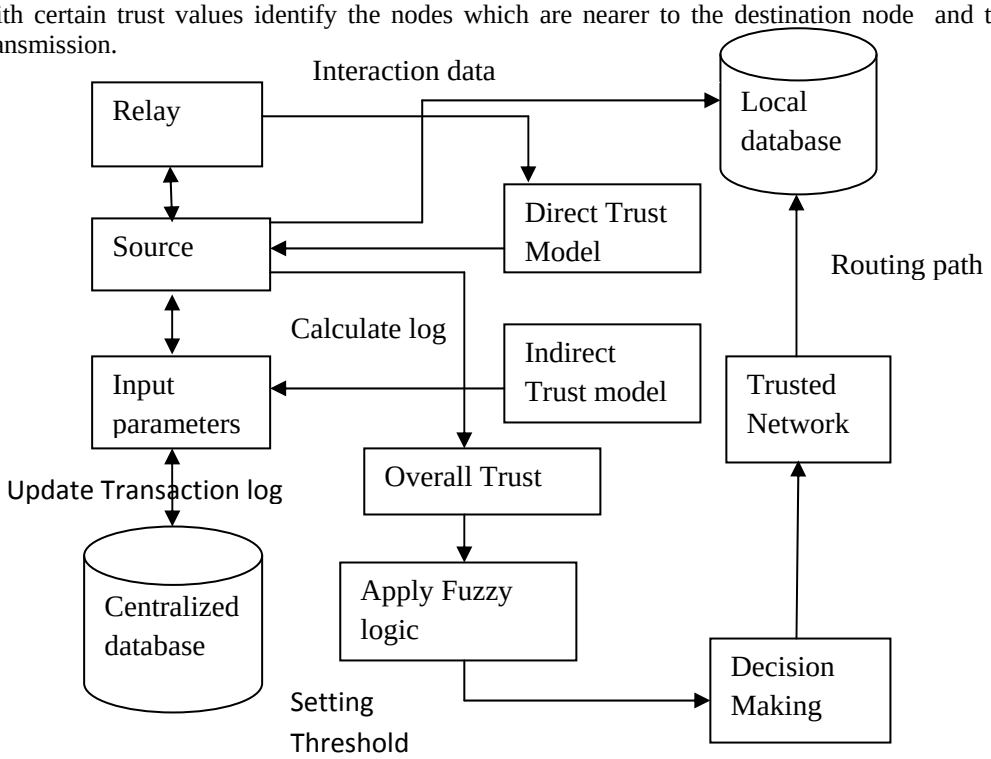

Fig.1. Flow diagram of Proposed work

Fig 1.Source node generates the log there by calculating the overall trust for that node. Then fuzzy logic is applied. By setting the threshold value decision making is done in order to transmit the packet in a trusted network. Centralized data contain the trust value for all the nodes. Each node stores its own log value in Localized data contains the log value of the node. So the packet can be sent through a trusted network. Each node compares its trust value with verge value if it is higher then that node consider as a trusted node.

III.B. METHODS

At first, the amount of trust in each sensor node is calculated so that sensor network can be used in a secure manner. Based on the calculated result, each sensor node come to conclusion that whether to communicate or not. The fuzzy logic [7] is implemented by using an AAMRP routing protocol. Ant colony optimization is used to find solutions for challenging problems it is helpful to find out the best paths through graphs.

Step:1 Sensor nodes are created.

Step 2:The nodes are communicating with each other to get the log of the neighbor nodes. Then the trust level is calculated.

Step 3:The trust level of the sensor nodes are calculated as follows:

Step:3.1 To calculate the trust level of sensor nodes, assume X as trustworthiness and Y as untrustworthiness.

Step:3.2 The X and Y are in the range of 0<=X<=1, 0<=Y<=1.

Step 3.3: Each sensor node has some estimation value, those values are cached in the base station.

Step 3.3: Estimation values are generated from the past actions

Step 3.4 The estimated values are sent from one association context to another.

1.Min : X = min(Xi,Xj),Min : Y = min(Yi,Yj)

2.Max: X = max(Xi,Xj),Max : Y =max(Yi,Yj)

So that the trust and untrust value can be calculated like this:

X = avg (Xi,Xj)/1-(avg(Xi,Yj)+avg(Xj,Yi))

Y = avg (Yi,Yj)/1-(avg(Xi,Yj)+avg(xj,Yi))

After calculating the max and min trust hold values compare the each node trusted value to the threshold value.

The node which has the higher value than the threshold value set as the trusted node. Then end the data packets to the destination through the trusted node.

IV. RESULTS AND ANALYSIS

The Nam class outputs at runtime in simulation setup :

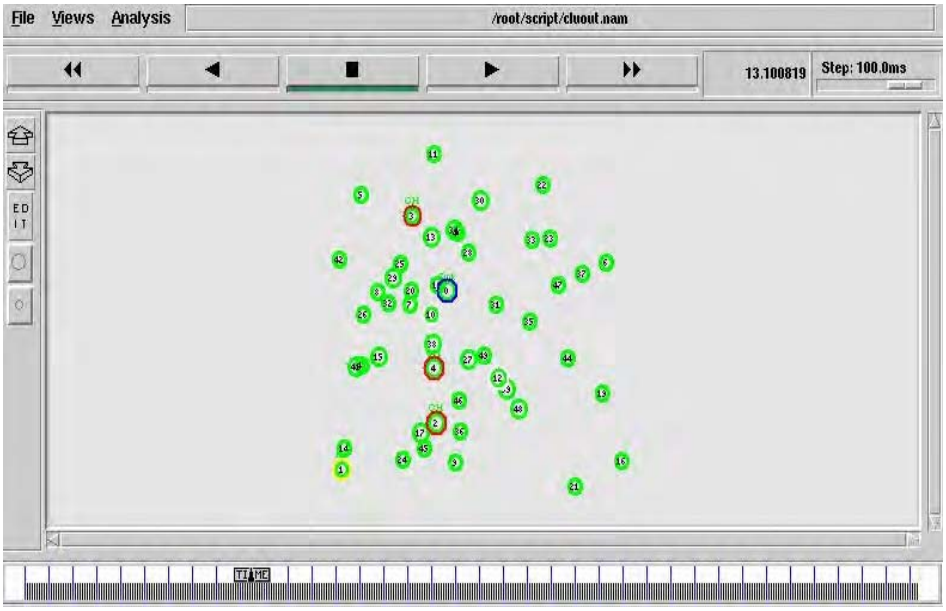

Fig.2. Node Deployment

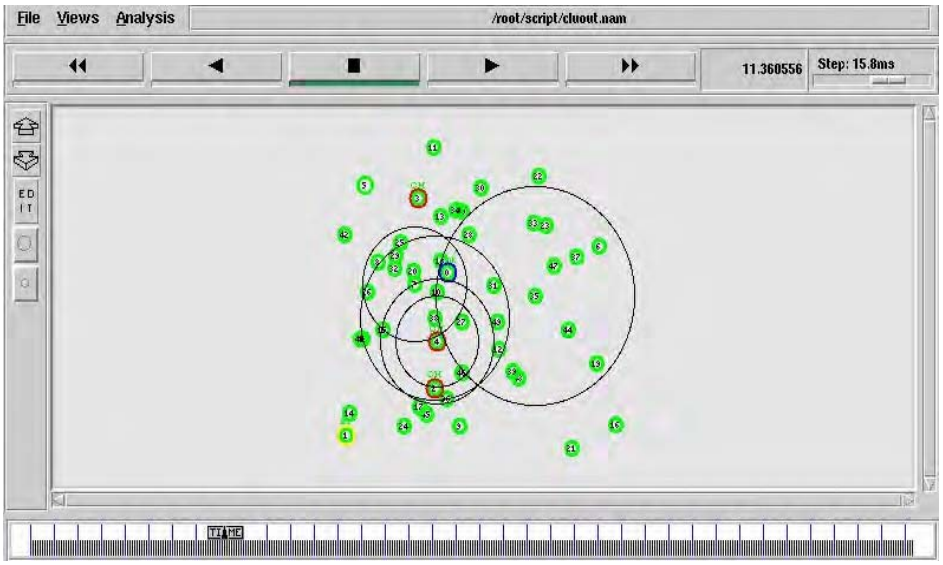

Fig.3. Node Communication

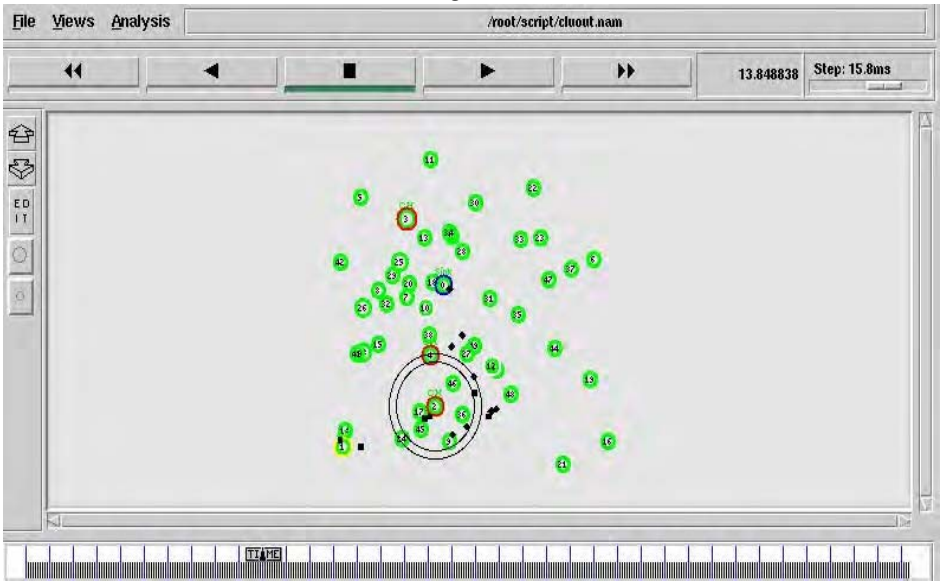

Fig.4. Packets sent through the trusted node.

InFig 2. The nodes are created. Node 2, node 3 and node 4 are the sender. Node 1is the wireless access point and node 0 is the sink node. In Fig 3. Nodes are communicating with each other in order to generate the log information. Thus the trust information is checked and shared. In Fig 4. Calculating the trust values and send the packets through trusted nodes

V. PERFORMANCE ANALYSIS

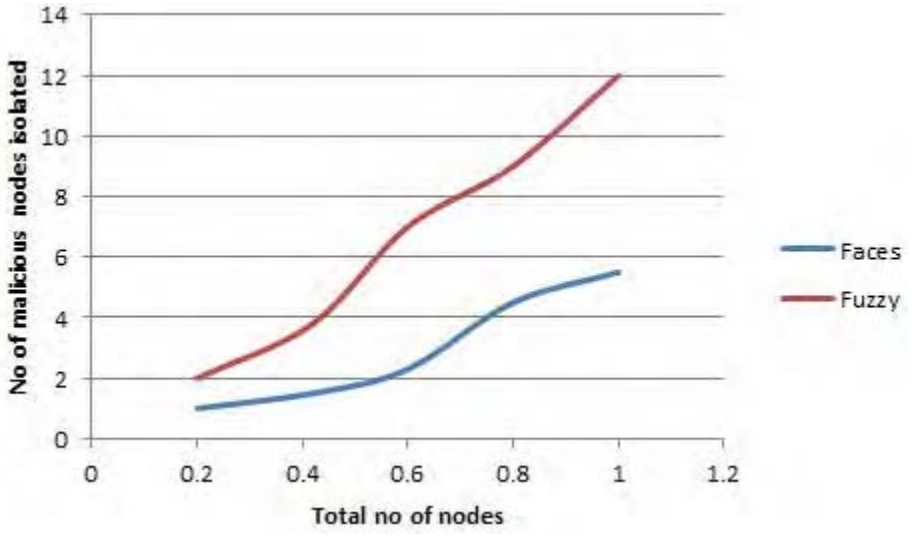

Fig. 5. Number of malicious nodes isolated versus total no of nodes

The stability of the reliable routing scheme is that find out by isolating the malicious node. In the Fig 5, By using rules fuzzy recognizes higher number of malicious nodes. When a trust value of the node is lower than the verge value, it is declared as minimum trusted node and isolated from the network. So we can accurately find out the malicious node. The existing multipath routing of the node depends mainly on the trust of a node which detection of the malicious node is not accurate. So to conclude that particular node is malicious itself it takes more time. Using fuzzy, more malicious nodes are detected accurately even in large no of nodes and it takes less time to find out the path, as more conditions could be done.

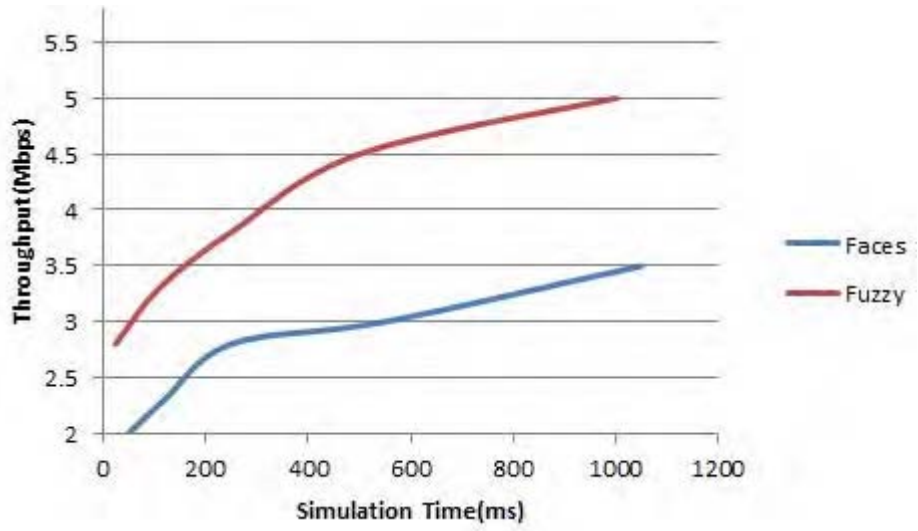

Fig.6. Throughput Versus simulation time

In Fig.6, Throughput is the mean of effectual packet delivery in a channel. We can see the throughput of fuzzy is maximum, means that a larger number of data packets can be transmitted from source to destination in a given amount of time.

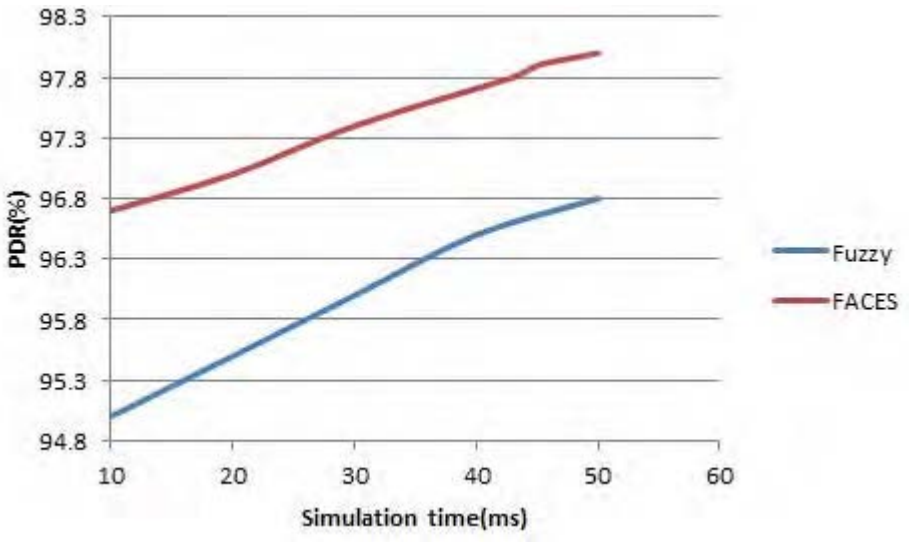

Fig.7. Packet dropped Versus simulation time

In the Fig.7, The packet drop is minimal in Fuzzy, means that the route which is accomadating malicious nodes can be effectively eliminated. The packet dropping rate is larger in other multipath routing protocols because the packets are routed through the misbehaving nodes. So when the number of nodes is increased , then the number of packet drop also gets increases.

VI. CONCLUSION

In this paper, For adequate and impervious communication, the fuzzy logic technique is designed to get trust model between the nodes in the wireless sensor network. The fuzzy logic is implemented by using aarmp routing protocol. We mainly concentrate on the trust values of each node that participating in the wireless network. Each node selects the trusted node by comparing the trust value of the nodes. The packets are sent through the nodes which have high trust values and nearer to the destination. So it finds out malicious node correctly when compared to existing approaches.

REFERENCES

[1] Chlamtac .,I , M. Conti and J.-N. Liu,2003. " Mobile ad-hoc networking: Imperativesand challenges, in *Ad-Hoc Networks*."New YorkElsevier, 2003, vol. 1, pp. 13–64, No. 1.

[2] Sung-Jib Yim, Yoon-Hwa Choi, 2012 ".Neighbor-Based Malicious Node Detection in Wireless Sensor Networks", in Wireless Sensor Network, 219-225.

[3] Sanjay Dhurandher .,K, Mohammad S. Obaidat,2011 "FACES: Friend-Based Ad Hoc Routing UsingChallenges to Establish Security in MANETs Systems", ieee systems journal, vol. 5, no. 2

[4] Idris Atakli.,M, Hongbing Hu, Yu Chen et al 2008. "Malicious Node Detection in Wireless Sensor Networks using Weighted TrustEvaluation", Proceedings of the 2008 Spring simulation multiconference.

[5] Rangarajan A. Vasudevan, Sugata Sanyal 2004. "Anovel multipath approach to security in mobile ad hoc networks (manets)",Proceedings of International Conference on Computers and Devices for Communication (CODEC'04), Kolkata, India.

[6] Jing-Wei Huang, Han-Chieh Chao and Obaidat,2011. " Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks" ,Inst. of Comput. Sci. & Inf. Eng., Nat. I-lan Univ., Ilan, Taiwan .

[7] Sanjay Dhurandher .,K, Vijeta Mehra, 2009. "Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks", International Conference on Advances in Computing, Control, and Telecommunication Technologies.

[8] Nithya.,S, R.Manavalan, 2012. "An Ant Colony Clustering Algorithm Using Fuzzy Logic", International Journal of Soft Computing And Software Engineering (JSCSE)e-ISSN: 2251-7545,Vol.2,No.5.

[9] Hallani.,H ,S. A. Shahrestani 2008. "Fuzzy Trust Approach for Wireless Ad-hoc Networks", School of Computing and Mathematics, University of Western Sydney, Australia.

[10] Suparna Biswas, Priyanka Dey 2012. "Trusted Checkpointing Based on Ant Colony Optimization in MANET",Third International Conference on Emerging Applications of Information Technology (EAIT), Department of Computer Science and Engineering, West Bengal University of Technology, Kolkata, India.

[11] Wei Gong, Zhiyang You et al 2009. "Trust Based Malicious Nodes Detection in MANET", Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China .

[12] Marjan Kuchaki, Rafsanjani, 2008. "Identifying Monitoring Nodes in MANET by Detecting Unauthorized and Malicious Nodes", Information Technology, Islamic Azad University Kerman Branch ,Kerman, Iran .