Eradication of Selfish Node in MANET Using CSNA Mechanism

[1]E.Janani, [2]D.Santhosh kumari, [3]A.Manimegalai
[1]PG Student, [2]Assistant professor, [3]Professor
[1]Department of ECE,
[1]Ganadipathy Tulsi's Jain Engineering college, Vellore, India

***Abstract* - MANET is a self-organizing system of mobile nodes without any fixed infrastructure. These mobile nodes act as an end system as well as a router. Most of the routing algorithms designed for MANET to forward every packet in the network. But in practice few of the nodes may act as the selfish nodes. Therefore, detecting these nodes is essential for network performance. In this paper, we present a new mechanism called categorized selfish node allowance to improve energy in wireless sensor networks to detect those selfish nodes. There is a possibility that because of less energy, the normal node will not respond to other nodes in the network. Since there is low energy for the node, there is a chance for the normal node to become dead when those nodes continuously respond to other nodes in the network. To avoid such situation, the normal node will act as selfish node. By calculating the energy for each node, the normal node will be differentiated from the selfish node**.

***Index Terms* - Selfish node, energy, cluster MANET**

I. INTRODUCTION

MANET is a group of mobile nodes that communicate with each other via wireless links either single hop or multi-hop to the destination nodes and here node will act as routers. The role of MANETs does not depend on pre-existing infrastructure or base stations. The nodes in MANETs are free to move randomly in any direction. As a result, the network topology of a MANET may change rapidly and randomly. All the network activities, such as discovering the topology and delivering data packets in the network, have to be executed by the nodes themselves, either individually or cooperatively. Depending on its application, the structure of a MANET may vary from a tiny and static network that is highly power-constrained to a large-scale, mobile and highly dynamic network. Most of the routing algorithms designed for MANET such as DSR [1] and AODV [2] are based on, that every node forwards every packet in the network. But some of the nodes may act as the selfish nodes. Those selfish nodes utilize the network resource and its services but they do not help to other nodes. Those nodes do not consume any energy such as CPU power or battery and bandwidth for retransmitting the data of other nodes and they reserve them only for themselves.

In an ad hoc network, selfish nodes may enter and leave the immediate radio transmission range at random intervals, may, collude with other selfish nodes to disrupt network activity and avoid detection [4], further complicating their detection due to the selfishness. Selfish nodes are inclined to get the greatest profits from the networks and at the same time these nodes trying to conserve their own resources like bandwidth [3], battery life or hardware. A selfish node only communicates to other nodes if its data packet is required to send to some other node and refuses to cooperate other nodes whenever it some data packets or routing packets are received by it that it has no interest in. Hence data packets are either refused to retransmit or are dropped for being received by a selfish node. Survey paper presents different methods that can be used to detect the selfish behaviour of some nodes in MANETS which find to save their resources like battery, CPU time, etc.

Various methods have been proposed for detection of selfish node in MANET by the researchers to address the problems. In general detection of selfish node is mainly based on communication of nodes in a network. [8] Detection and deletion of selfish node by Distributed and Co-operative approach. Distributed approach which forces every neighbour node to find the selfish node and the Co-operative approach is used to re-introduce the detected node, here the network performance is improved but network delay is increased. [7] Detection of node misbehaviour is based on link behaviour, they proposed two technique (2ACK & PCF) to detect selfish node which will be used parallel. 2ACK detect the misbehaviour link by acknowledgement by destination and then Principle of Conservation of Flow (PCF) is used to detect the selfish node in that link, here processing time is reduced but 2ACK technique, sometimes destination node will acknowledged only some information of data packets. [10] Enhanced node co-operation technique is proposed to outwitting the selfish node which is hybrid technique of reputation based and incentive based mechanism, here reputation based scheme is used to detect selfish node and incentive based scheme encourage the detected node to co-operate to other nodes in a network. [9] Identification and elimination of selfish node by credit based system, here all the nodes in a network are initialized with same credit and that credit will increase or decrease based on the packet transferred successfully or not. It has disadvantage that detected nodes are not introduced. This method also presents different activities of selfish nodes and their collisions on MANET. [11] Detecting and eliminating selfish node in MANET by Token Based Umpiring Technique (TBUT), where every node need token to participate in the network. Neighbouring node act as umpire to detect the selfish node, here the limitation is booking of innocent node as selfish node.

The paper is organized as follows: Section 1 provides an introduction to mobile ad hoc network, Section 2 explains a brief overview of DSR routing protocol, Section 3 provides proposed system details, Section 4 summarizes our simulation results, Section 5 concludes our proposed work, Section 6 gives information about future work and Section 7 includes relevant references.

II. DSR ROUTING PROTOCOL

Routing protocol in MANET required to deal with the movements of nodes in an in-deterministic manner. In this paper on-demand Enhanced-DSR routing protocol is proposed. It is based on the concept of source routing. [1] Mobile nodes are required to maintain route cache table that contains the source routes of which the mobile is aware. A source node which needs to communicate with a destination node, will first examine its own route cache table.

The protocol is divided into two main functions:

A. Route discovery

B. Route maintenance

A. Route discovery

If the route to the destination is expired then, it will start the process for Route discovery by broadcasting a RREQ (Route Request) packet to its neighbours. Each intermediate node receive the RREQ and adds its address to the RREQ and then re-broadcast the modified RREQ. If the destination node received the RREQ message from the source node then it will create a RREP (Route Reply) packet and transmits the RREP back to the source node by using the accurate reverse path. When the source node receiving the RREP, it will updates its route cache with an entry for the destination node and it starts sending the data packet.

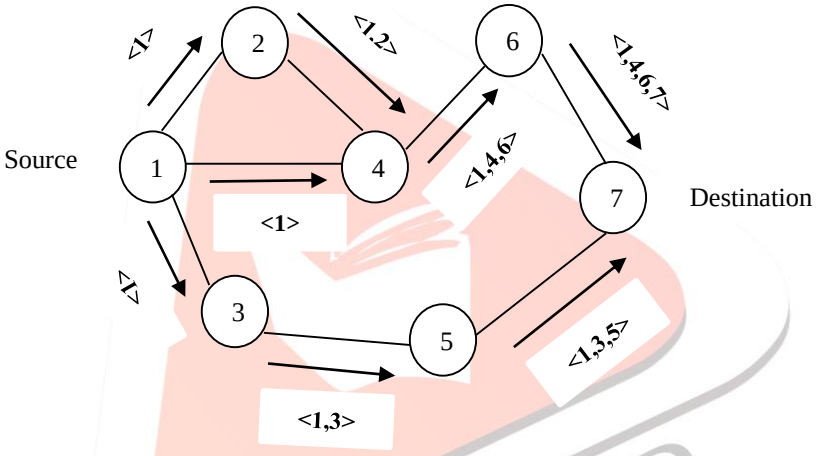

Fig .2.a Building Record Route during Route Discovery

B. Route maintenance

On the other hand route maintenance is used to handle path break. If a node identify there is a link break from data link layer, it will create a RERR packet and send back to the source node using the part of the information of route traversed so far. The notified source node must delete the path break link from its route cache table. If the source node need to send another packet to the same destination, it must try another route discovery process again if it does not have any other routes.

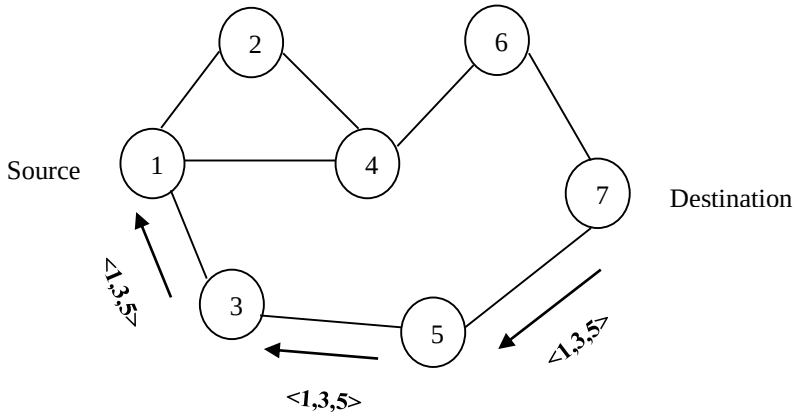

Fig .2.b Propagation of Route Reply with the Route Record

III. PROPOSED SYSTEM

The main purpose of our paper is to address and analyze the impact of selfish behavior of nodes. Limited resources are available in MANET and the presence of selfish node that utilizes the network resources but refuses to forward a packet. Because of these reasons the network performance is decreased. The ultimate goal of our proposed system is to accurate detection of selfish node and to improve the network performance and efficient utilization of resources this paper implementing Clustered MANET based on node communication and categorized selfish node allowance mechanism.

A. Clustered MANET

In this scheme the detection of selfish nodes done by creating a Clustered MANET and calculating the node communication ratio. Clustered MANET consists of Cluster Head, Cluster Member and Cluster Gateway. The group of nodes which are in same communication range are combined to form cluster is shown in Fig 3. Cluster Head is selected for every cluster group with the node having highest communication ratio. The nodes which are all present in the Cluster group are the Cluster Members and the node which common between two cluster groups is known as Cluster Gateway. After the formation of Cluster group, calculate the communication ratio for all node in the network. Then the cluster head is selected by which has highest node communication ratio (NCR). And the next process, is to detect the selfish node based on NCR. Therefore by calculating the energy for those nodes, more number of nodes is detected from the selfish nodes and those nodes can be used for future transmission in the network. Depending upon the nodes in the network with its communication range the nodes are combined to form clusters in the network. Initially the cluster head is selected based on node communication ratio. Upon communication within each clusters in the network, the selfish nodes are gathered together. If the range of NCR is found to be greater than 30%, it is a normal node which is able to transmit and get information. If the range of NCR is found to be lesser than 30%, then the node is a selfish node.

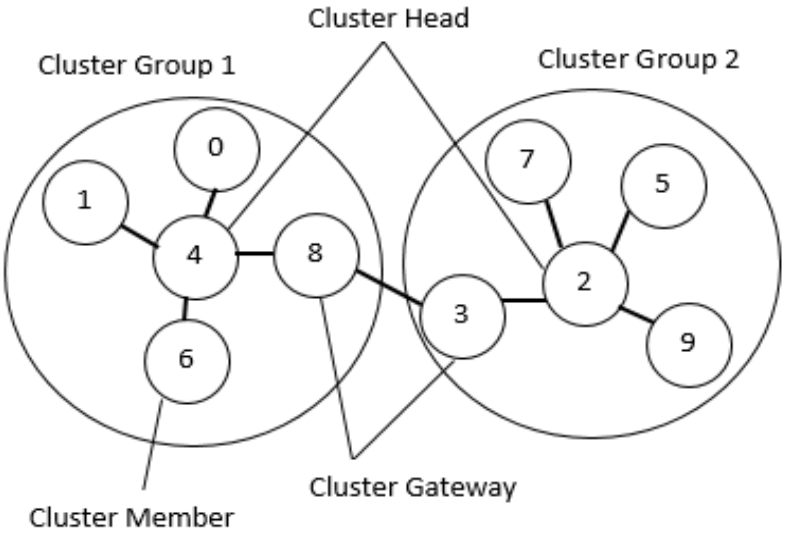

Fig .3 Formation of Cluster group

B. Equation for Node Communication Ratio

The NCR is computed depending upon the route request sent and route reply received messages within the communication range of the node. For a node in the network, the NCR is calculated by the ratio of difference among the number of route request sent and the number of unsent route reply messages to the total number of route request message sent.

The node communication ratio (NCR) is calculated by,

$$NCR = \frac{(P-R)}{P} * 100 \quad (1)$$

Where,

R = P – Q
P- No. of RREQ sent
R- No. of RREP unsent
Q- No. of RREP received

Once the NCR is calculated for all the nodes in a network then which has highest communication ratio that node is selected as cluster head in each group.

C. CSNA Mechanism concept

Now the concept of energy is introduced in the proposed work. First assign a list for the nodes that are detected as selfish one. If a node is not responding in the network, then it's not cent percent guarantee that it is a selfish node. There can be other reasons as well regarding the misbehavior nature of the network. Every node in the network will have a certain amount of energy. If the node has

sent more data, there is possibility that the node might have lost its energy less than the threshold value. If again the node keeps on sending data, there is a probability that the node will lose all its energy and become dead. So when the node has minimum amount of energy, that node instead of being in a dead condition, it avoids sending reply to the other nodes in the network. The flowchart for the above process is shown in Fig 4. The energy levels are compared with the threshold energy levels. If the energy level is less than the threshold value, the node is said to be weak node. The information about the node is passed to rest of the nodes and the node is removed from the current transmission and the node can be used for future purpose. If the energy level is greater than the threshold value (Th), the node is known as selfish node.

The below flowchart explains how to separate the normal node and selfish node. For that first list out the detected selfish node by the NCR. Then the energy level of those nodes are calculated and compared with the threshold energy. If it is normal node then it is removed from the current transmission otherwise it is removed from the entire routing list. The information about the selfish node is passed to rest of the nodes and the node is removed from the entire transmission in the network. Therefore the energy values are calculated for the nodes that are found as selfish in the network. The rate at which energy is consumed in the network by individual sensor nodes is defined by the energy model.

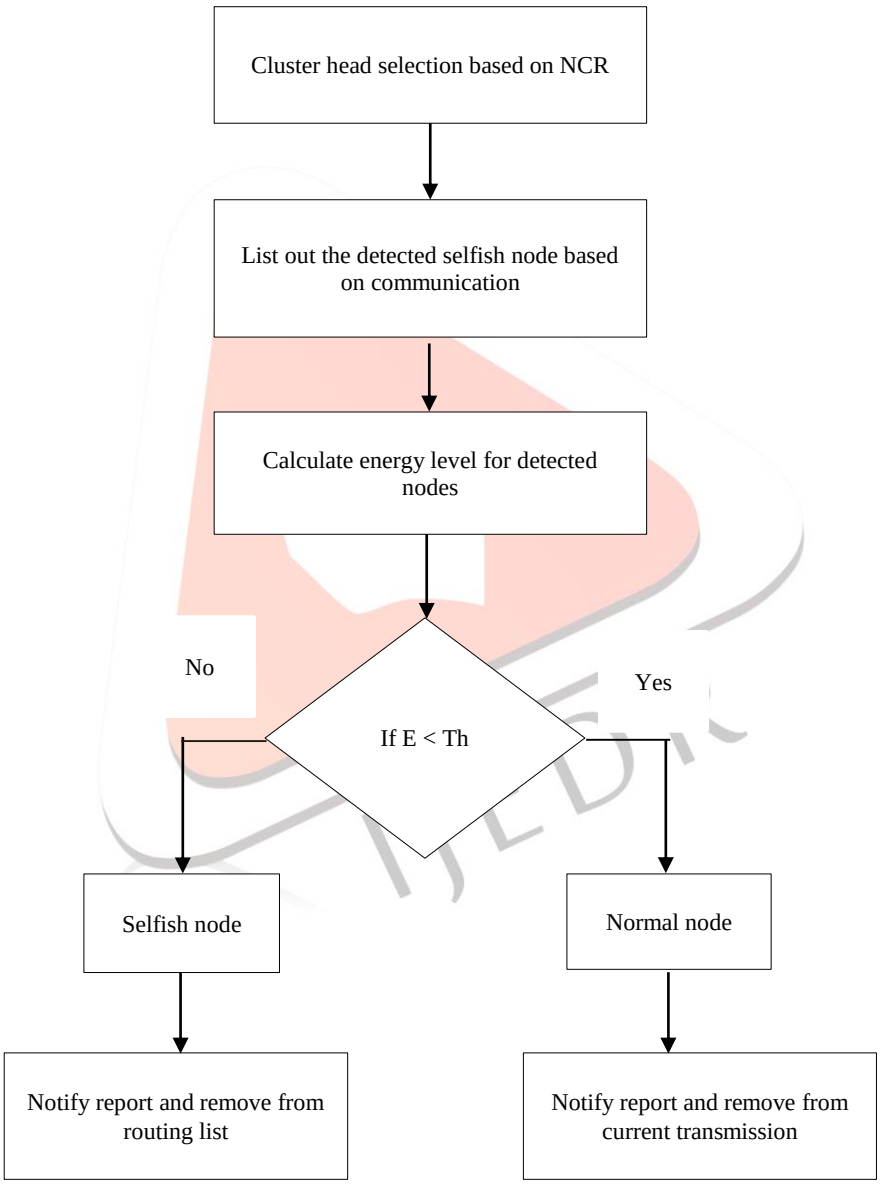

Fig .4 Flowchart for identification of selfish node

D. Equations for Energy Calculation

The energy consumed by a node in the network is shown in below equation,

$$E_C = E_t + E_r + E_i \quad (2)$$

The basic equation to find the remaining energy in the network is shown below equation,

$$E_R = E_I - E_C \quad (3)$$

Where,

E_R - Remaining energy
E_t - Energy consumed for transmission
E_I - Initial energy
E_r - Energy consumed for reception
E_C - Consumed energy
E_i - Energy consumed during ideal

IV. SIMULATION RESULTS

Network simulator (NS2) is used to analyze the performance of the proposed scheme. It is an open source programming language written in both the C++ and Object Oriented Tool Command Language. NS2 is an isolated event time driven simulator which is mainly targeted to model the network protocols. The nodes are randomly distributed in the simulation environment and those nodes have to be configured as mobile nodes by using the node-configuration command in NS2. The parameters which are all used for the simulation of the proposed scheme is tabulated below. The simulation of the proposed scheme is deployed by 38 nodes in the simulation area 1000×1000. The nodes are moved randomly in any direction within the simulation area by means of the mobility model Random way point as shown in Table 1. The nodes are communicated with each other within the communication range by using the communication protocol User Datagram Protocol. The traffic is controlled by using the traffic model CBR. The radio waves are broadcasted by means of the propagation model two ray ground wave propagation. Omni directional antenna is used in the simulation because all the nodes need to accept the signal from all direction.

Table 1 Simulation Parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	50 ms
Number of nodes	38
MAC type	802.11
Traffic model	CBR
Transmission range	250m
Network interface Type	WirelessPhy
Mobility Model	Random Way Point

A. Throughput

Throughput is the average of successful messages delivered to the destination. The average throughput is estimated using the equation is given below.

$$\text{Throughput} = \frac{\sum_0^n packets\ received\ (n) * packet\ size}{1000} \quad (5)$$

The performance of the proposed scheme is estimated by the throughput using network simulator. The graph plotted between the throughput and simulation time (ms).

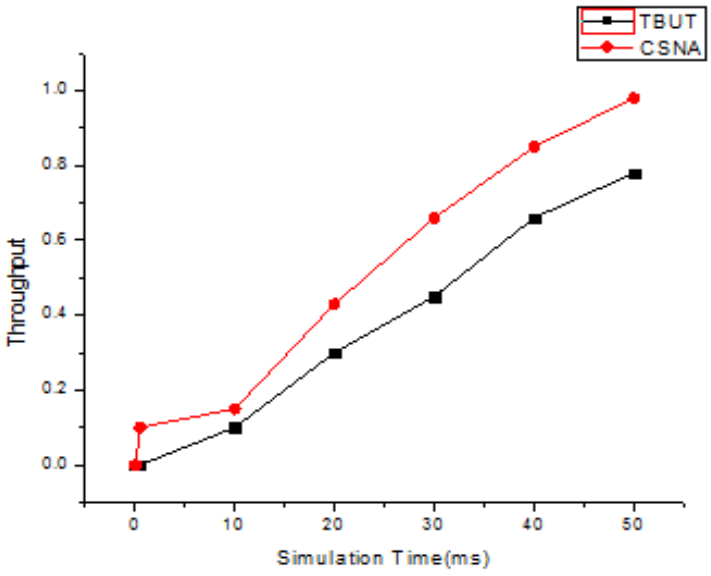

Fig .5 Throughput V_S Simulation Time (ms)

B. Simulation of NAM window

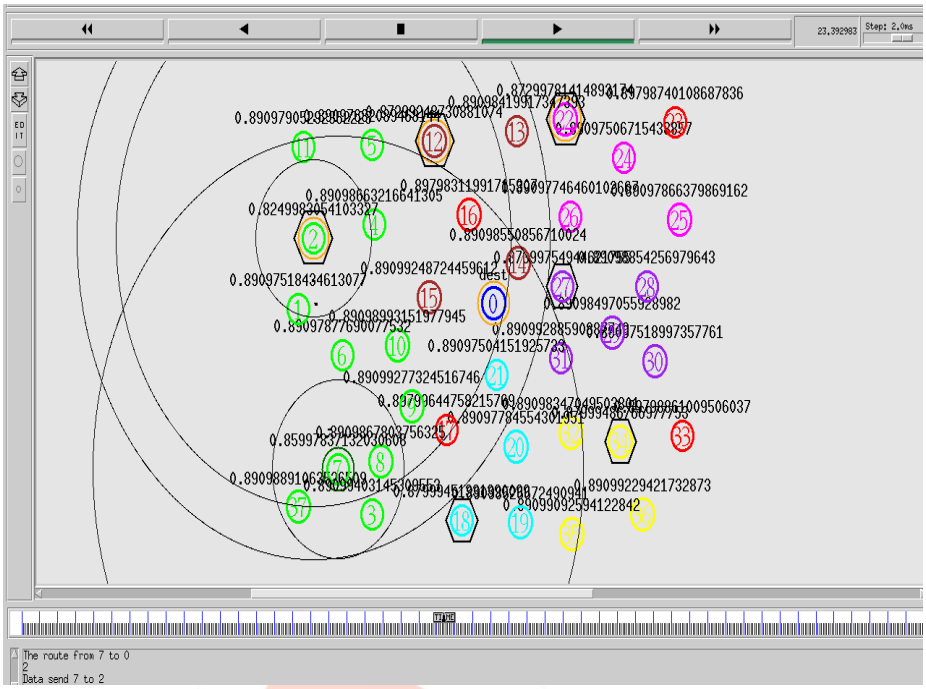

Fig .6 NAM window

In Fig .6 shows the animation of the proposed scheme here totally six cluster group are generated by its communication range and the cluster head is represented in hexagon shape. The red colour nodes are detected as selfish node based on the CSNA mechanism. And that nodes are removed from the entire routing list. Then the routing process is done efficiently without the selfish node and the throughput is increased compared to existing scheme. Removal of selfish node in the network give secure transmission.

V. CONCLUSION

Mobile Ad Hoc Networks have an effective research area over the past few years due to their possibly widespread application in military and civilian communications. Existing method are only concentrate on co-operation of node in the network to detect the selfish node. So here normal node with low energy is assumed as selfish node. In this paper the proposed scheme successfully executed and analyses about the detection of selfish node by calculating the energy level of each node so therefore normal node and selfish node is separated. After the separation the selfish nodes removed from entire routing list. And the network throughput and secure transmission is estimated using NS2.

VI. FUTURE SCOPE AND ENHANCEMENT

MANET become effective only when the detected nodes are re-entered in to the network. Whenever there is an insufficient number of nodes for packet transmission then the detected nodes are re-entering in to network with full co-operation. For that Revival of selfish node in clustered MANET (RSC) is the enhancement scheme for re-establishment of detected nodes in the network.

REFERENCES

[1] Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5. 2001.

[2] D.Ian Chakeres and M. Elizabeth Belding-Royer, “AODV routing protocol implementation design” Proceedings of the International Workshop on Wireless Ad Hoc Networking, Tokyo, Japan, March 2004.

[3] Wu, Lien-Wen, and Rui-Feng Yu. "A threshold-based method for selfish nodes detection in manet." Computer Symposium (ICS), International. IEEE, 2010.

[4] P. Brutch and C. Ko. “Challenges in intrusion detection for wireless adhoc networks”. In proc. of the IEEE Symposium on Applications and the Internet (SAINT) Workshop, 2003.

[5] G. Bo Yong, C. Jian, and U. W. Pooch, "Detecting blackhole attack in mobile ad hoc networks, " in Personal Mobile Communications Conference, 5th European (Conf. Publ. No. 492), 2003.

[6] V.Pavani , T.Rama Mohan , A.Vijay Kumar “Managing selfish nodes through node cooperative incentives in manets”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol.2, Issue 9, September 2013.

[7] Samreen, S.; Narasimha, G., "An efficient approach for the detection of node misbehaviour in a manet based on link misbehaviour," Advance Computing Conference (IACC), IEEE 3rd International, vol., no., pp.588, 592, 22-23 Feb. 2013.

[8] Tarannum, R.; Pandey, Y., "Detection and deletion of selfish manet nodes-a distributed approach," Recent Advances in Information Technology (RAIT), 1st International Conference on , vol., no., pp.152,156, 15-17 March 2012.

[9] Sheetal J. Nagar, Divan G. Raimagia, Pinaki A. Ghosh "Identification and elimination of selfish nodes in adhoc network," International Journal of Engineering Research and Development, Volume 10, Issue 4, April 2014.

[10] Rekha Kaushik, Jyoti Singhai "Enhanced node cooperation technique for outwitting selfish nodes in an ad hoc network," Institution of Engineering and Technology (IET Networks) 2014.

[11] Jebakumar Mohan Singh Pappaji Josh Kumar, Ayyaswamy Kathirvel, Namaskaram Kirubakaran, Perumal Sivaraman and Muthusamy Subramaniam, "A unified approach for detecting and eliminating selfish nodes in manets using TBUT," EURASIP Journal on Wireless Communications and Networking 2015.