*International Journal of Research in Advent Technology (IJRAT) Special Issue*
*E-ISSN: 2321-9637*
*Available online at www.ijrat.org*
*International Conference "*INTELINC 18*", 12th & 13th October 2018*

# A Scattered for detecting selfish nodes in MANET using Collabrative watchdog Algorithm

R.Mangayarkarasi, Dr.R.Manikandan Ph.d.
*Computer Science and Engineering, Assistant Professor /Programmer in CSE, Annamalai University, Department of Assistant Professor, Computer Science and Engineering,Government college of Engineering,Dharmapuri,*
mangay2014@gmail.com, rmkmanikandan@yahoo.co.uk.

**Abstract-** A mobile ad hoc network (MANET) is a self-organized system comprised by multiple mobile wireless nodes. The node misbehavior due to selfish reasons can significantly diminish the performance of MANET. A selfish node attempts to use the resources only for its own purpose and it hesitates to share the resources with their neighbors. So, it is very important to detect the selfish nodes to improve the performance of MANET. Initially, an architectural model of a MANET is constructed and the communication between the mobile is originated. The packet drop can happen in MANET due to the selfish node or network congestion. In this paper, a distributed global trust is presented to improvise the detection of selfish node in the network in MANET and then This paper studies the impact of selfish nodes concentration on the quality of service in MANETs. The main reason for using trust and reputation in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The simulation study demonstrate the proposed method enhances the selfish node detection ratio , packet delivery ratio(PDR), and average packet drop ratio, Quality of service.

**Keywords:** Mobile ad hoc network (MANET); Selfish node; Route discovery;

Route request (RREQ); Packet delivery ratio (PDR); Trust management, Reputation system, Quality of service .

## 1. INTRODUCTION

Mobile ad hoc network (MANET) is a wireless network among mobile devices. It is a self-configuring system of mobile nodes connected by wireless links, which contains a network area with nodes. This network is relatively a new communication paradigm, which contains a group of mobile devices communicating through awireless medium. A major problem in MANETs is the frequent occurrence of network divisions due to the unlimited movement of the mobile nodes in the network. This results in some data getting inaccessible to some of the nodes. Thus, data accessibility needs to be considered carefully in MANET [1]. Each mobile node in MANET requires the help of other nodes to forward the packets. The nodes are expected to wait for a pre-defined time interval between successive transmissions. But a mobile node may misbehave due to network congestion and selfishness. Node misbehavior due to selfish or malicious reasons or faulty nodes can significantly reduce the performance of MANETsNode misbehavior means deviation from the original routing and forwarding. The source node can relay packets to the destination node through other nodes in MANET. The selfish nodes [2] do not participate in the routing process, which intentionally delay and drop the packetThese misbehaviors of the selfish nodes will impact the efficiency, reliability, and the fairness. A selfish node does not perform the process related to packet forwarding function for data packets unrelated to itself. The selfish node utilizes its limited resources only for its own purpose because of the energy and storage constraints for each node inthe MANET. It aims to save its resources to theEssentially, watchdog systems overhear wireless traffic and analyse it to decide whether neighbour nodes are behaving in a selfish manner. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behaviour of the system. Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. In this case, the effect can

even be more harmful, since these nodes try to intentionally disturb the correct behaviour of the network. For example, one harmful malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. Malicious nodes are hard to detect using watchdogs, as they can intentionally participate in network communication with the only goal to hide their behaviour from the network. Thus, since we assume that these nodes may be present on the network, evaluating their influence becomes a very relevant matter. In this paper, a distributed trust is presented to improvise the detection of selfish node in the network in MANET. The main reason for using trust and reputation in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The simulation study demonstrate the proposed method enhances the selfish node detection ratio , packet delivery ratio(PDR), and average packet drop ratio. maximum, so this type of misbehaving node discardsall incoming packets except those which are destined to it. The selfish nodes neglect to share their resources, such as battery power, CPU time, and memory space to other nodes in MANET. This behavior is observed in the data link/MAC layer, which is decisive, specifically when the mobile nodes possess small residual power.

The features of the selfish nodes are as follows:

_ Non-participation in routing

_ No transmission or reply to HELLO messages

_ Intentional postponement of route request (RREQ) packets

_ Data packet dropping Managing trust [3] in a distributed MANET is achallenging and critical task to achieving mission andsystem goals such as reliability, scalability, availability ,and reconfigurability. Trust management contributes aunified approach for interpreting and specifying security policies, credentials, and relationships. It involves [4] trust establishment, trust revocation, and trust update in MANET. The trustworthiness is evaluated using the trust information or evidence, which is difficult due to changes in topology induced by node mobility or node failure. In this MANET framework, the nodes areconnected to the network, which are monitored by a server agent, and theMANET architecture is shown in Figure 1. It manages the details of the mobile nodes in a network like

_ Behavior of the node

_ Speed of the node

_ Direction of the node

_ Position of the node

Previous works have demonstrated that in RTBD are appropriate mechanisms to detect misbehaving and selfish nodes.Essentially, watchdog systems overhear wireless traffic and analyse it to decide whether neighbour nodes are behaving in a selfish manner. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behaviour of the system. Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. In this case, the effect can even be more harmful, since these nodes try to intentionally disturb the correct behaviour of the network. For example, one harmful malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. Malicious nodes are hard to detect using watchdogs, as they can intentionally participate in network communication with the only goal to hide their behaviour from the network. Thus, since we assume that these nodes may be present on the network, evaluating their influence becomes a very relevant matter. In this paper, a distributed trust is presented to improvise the detection of selfish node in the network in MANET. The main reason for using trust and reputation in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The simulation study demonstrate the proposed method enhances the selfish node detection ratio , packet delivery ratio(PDR), and average packet drop ratio

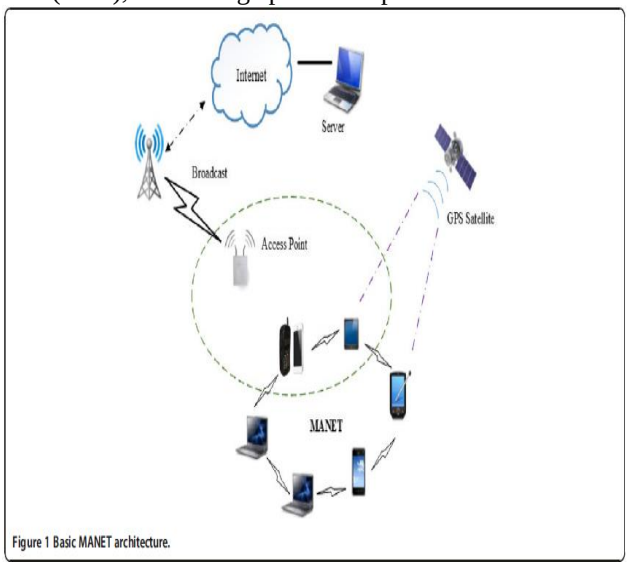


Figure 1 Basic MANET architecture.

## 2. ARCHITECTURE OVERVIEW

A selfish node usually denies packet forwarding in order to save its own resources. This behaviour implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behaviour is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being re-transmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not). An example of how collaborative contact based watchdog works is outlined in figure 1. It is based on the combination of a local watchdog and the diffusion of information when contact between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about this positive (or negative) detections.

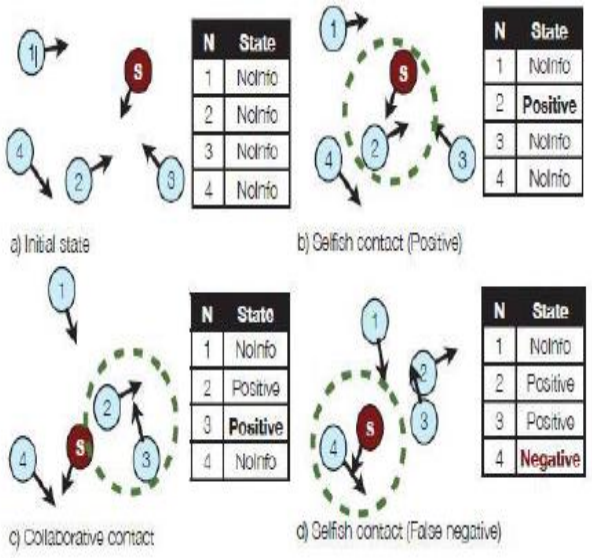


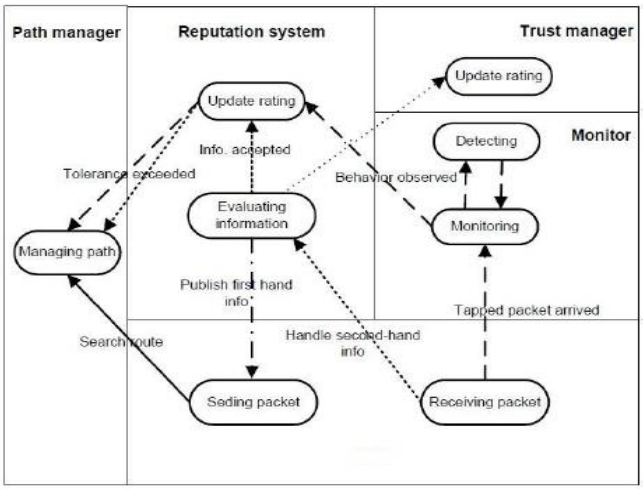

**Fig. 2: An example of how collaborative contact based watchdog works.**

a) Initially all nodes have no information about the selfish node.

b) Node 2 detects the selfish node using its own watchdog.

c) Node 2 contacts with node 3 and it transmits the positive about the selfish node.

d) The local watchdog of Node 4 fails to detect the selfish node and it generates a negative detection (a false negative).




In figure 3 is enhanced work to the collaborative contact based watchdog system which detect the selfish node in the network by using watchdogs and second hand information , the second hand information is receive from the others node's watchdog . In above figure the Monitoring part is done by the watchdogs for detection node's selfishness behavior, if watchdog finds node is behave selfishness in the network then the Reputation system decreases the node's reputation, Trust manager is maintain the global trust of the node in the network which is used to improve the detection of selfish node in the network , if node's global trust is below the threshold value then Monitor easily detect the selfish node .

The dashed lines describe how the first hand information is collected. When a node i receives a packet from j ,then i's watchdog whether it is passive acknowledgment packet, if it is, the rating about j will be updated . If the reputation rating is greater than misbehaved threshold, it will inform Path manager to delete all the paths that contains the node j from the route cache of node i.

The dotted lines describe how second hand information published by the other nodes is handled. As seen in the figure, when node i receives published information it passes the information to the Reputation system to decide

whether it should be accepted. If the information is accepted, the ratings about node j are updated. If the reputation rating after updating exceeds tolerance threshold, all the paths that containing the node j will be deleted from Path manager.

**A. Bayesian Estimation**

Bayesian estimation is a statistical procedure which endeavors to estimate parameters of an underlying distribution based on the observed distribution . Given a prior belief of the probability of some event happens, information that is acquired at each observation is update to reflect the added knowledge and to increase the precision of the belief. Equation 1 shows the Baye's theorem.

$$p(\theta_i|y) = \frac{p(y|\theta_i)P(\theta_i)}{\sum_{i=1}^{n} p(y|\theta_i)P(\theta_i)}$$

Equation-1

Following example explains the meaning of the equation as well as illustrates how Bayesian analysis is used to predict the probability whether a node misbehaves or not. Suppose in the MANET a node i has never met node j before. i has a hypothetic prediction P(θi) about the probability of whether node j will misbehave or not. Here θi is the model parameter representing a node misbehaves or behaves well. P(θi )is the prior distribution which means a probability of θi before any data have been observed. After I has communicated with j, i gets observed data y about j. Then we can know p( y| θi) a probability of the data y given a know parameter θi .

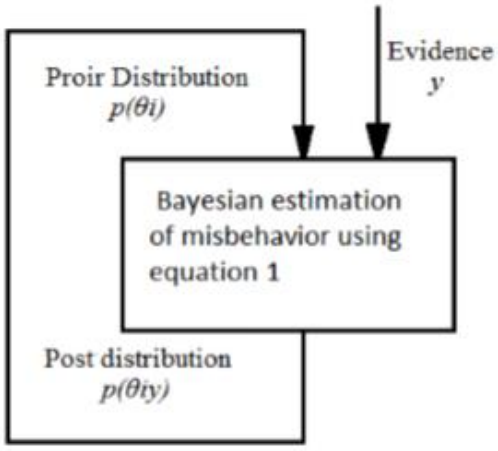



**Fig4: Bayesian estimation of misbehavior**

However, what we want to estimate is the probability of iθ given observed information y. It is called posterior distribution and expressed as p( θi | y) . With Equation 1, we can see that p(θi | y) can be calculated if P(θi )and p(y | θi )are known. After p(θi | y) is calculated, it will be used as the prior distribution in the next interaction. This approach of estimating a belief using Bayesian analysis is illustrated in Figure 4.

**Proposed Algorithm**

Step 1: Start
Step 2: Initialize two nodes as selfish nodes and two nodes as malicious nodes
Step 3: Find one hop neighbors for all nodes in network
Step 4: Initial Local watchdog system monitors node behavior
Step 5: Every Node will also receive indirect information about selfish nodes.
Step 6: Initially Local Watch dog system assigned NOINFO and this will be updated when a node finds a selfish node
Step 7: If a nodes finds its neighbor as selfish, then POSITIVE
Step 8: If a malicious nodes lie about selfishness then it will send NEGATIVE
Step 9: If a node found nothing then it will send NOINFO
Step 10: Indirect information is calculated
Node Reputation Calculation:
Node reputation = Local watchdog info + indirect info
Local watchdog info

= +2 (if positive detection)
= -2 (if negative detection) Indirect info
= +1 (if positive detection)
= -1 (if negative detection)
= 0 (if Noinfo)

Step 11: Routing is done between source and destination, avoiding selfish nodes in routing path

## 3. SIMULATION RESULT

### A. Simulation Environment

We performed our simulation using separate event network simulator ns2.34. Our network scenario consists of randomly placed 40 nodes within 2000 x 2000 m area. Simulation time was 720 seconds. Nodes were use 2-Mbps transmission rate with transmission range 250-m as we used IEEE 802.11 for MAC protocol. Data packet rate was 512bytes. We used AODV network layer multicast routing protocol with its default routing parameter values. We used one receiver with one sender and source sends packet with size 512 bytes. Attackers are randomly placed and randomly activated in order to imitate arbitrary nature of malicious node.

### B. Performance Analysis

Following graph shows the packet loss, packet delivery ratio and end to end delay in the network. Figure 4 shows the packet loss in the network. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

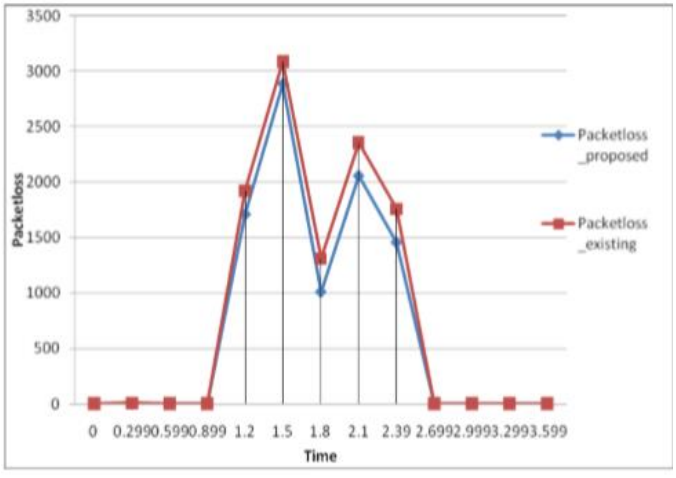



**Fig 5: Graph of packet loss**

**Figure 6 shows the packet delivery ratio (PDR) of project build to detect selfish node in the network**

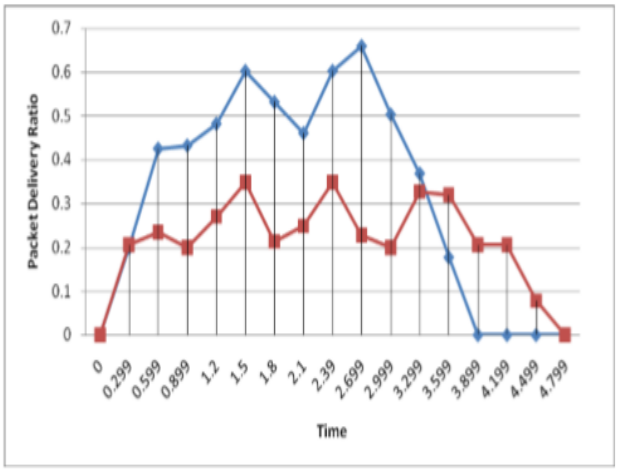



**Fig6: Gragh of Packet Delivery Ratio**

**Figure 7 shows the end to end delay which is one-way delay refers to the time taken for a packet to be transmitted across a network from source to destination.**

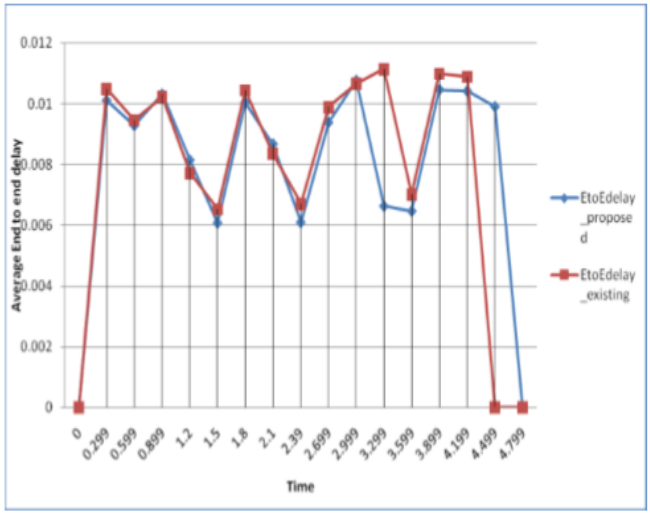
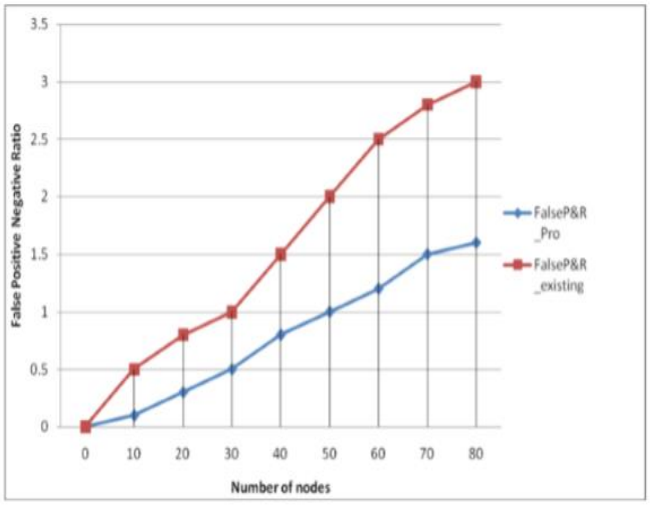



**Fig7:Graph for End to End delay**

**Figure 8 shows the false positive and false negative ratio in the network.**




## 4. CONCLUSION

The misbehavior of selfish nodes is a major problem in MANET. The selfish nodes do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviors of the selfish nodes will impact the efficiency, reliability, and fairness. The selfish node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET. This study proposes a new technique, namely RTBD, to detect the selfish nodes in an efficient manner. The suggested RTBD method is an effective method, which enhances the performance of MANET.In the proposed mechanism, each node independently monitors the packet forwarding behavior of its neighbors. A cooperative mechanism is utilized among the nodes in the same neighborhood for detection of selfish or malicious nodes. The mechanism is simulated in network simulator and the results show that the scheme is highly robust, efficient and has improved performance mechanisms.

## REFERENCE

[1] Jae-Ho C, Kyu-Sun S, SangKeun L, Kun-Lung W: Handling selfishness in replica allocation over a mobile ad hoc network. IEEE Transactions on Mobile Computing 2012, 11: 278-291.

[2] Ryu BG, Choi JH, Lee S: Impact of node distance on selfish replica allocation in a mobile ad-hoc network. Ad Hoc Netw. 2013, 11: 2187-2202. 10.1016/j.adhoc.2013.05.001

[3] Sedghi H, Pakravan MR, Aref MR: A misbehavior-tolerant multipath routing protocol for wireless ad hoc networks. Int J Res Wireless Syst 2013, 2(2):6-15.

[4] Mejia M, Peña N, Muñoz JL, Esparza O, Alzate MA: A game theoretic trust model for on-line distributed evolution of cooperation in MANETs. J. Netw. Comput. Appl. 2011, 34: 39-51. 10.1016/j.jnca.2010.09.007

[5] Singh R, Singh P, Duhan M: An effective implementation of security based algorithmic approach in mobile adhoc networks. Hum Centric ComputInfSci 2014, 4: 1-14. 06/19 2014 10.1186/2192-1962-4-1

[6] Hernández-Orallo E, Olmos MS, Cano J-C, Calafate C, Manzoni P: A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. Wirel. Pers. Commun. 2014, 74: 1099-1116. 02/01 2014 10.1007/s11277-013-1346-y

[7] Manoj V, Raghavendiran N, Aaqib M, Vijayan R: Trust based certificate authority for detection of malicious nodes in MANET. In Global Trends in Computing and Communication Systems. vol. 269. Edited by: Krishna PV. Springer, Berlin; 2012:392-401.

[8] Jawhar I, Trabelsi Z, Al-Jaroodi J: Towards more reliable and secure source routing in mobile ad hoc and sensor networks. Telecommun. Syst. 2014, 55: 81-91. 10.1007/s11235-013-9753-7

[9] Rodriguez-Mayol A, Gozalvez J: Reputation based selfishness prevention techniques for mobile ad-hoc networks. Telecommun. Syst. 2013, 1-15.

[10] Afghah F, Razi A, Abedi A: Stochastic game theoretical model for packet forwarding in relay networks. Telecommun. Syst. 2013, 52: 1877-1893. 10.1007/s11235-011-9471-y

[11] Hernandez-Orallo E, Serrat MD, Cano JC, Calafate CT, Manzoni P: Improving selfish node detection in MANETs using a collaborative watchdog. Commun Letters IEEE 2012, 16: 642-645.

[12] Padiya S, Pandit R, Patel S: Survey of innovated techniques to detect selfish nodes in MANET. IJCNWMC 2013, 3(1):221-230.

[13] Roy DB: R Chaki, MADSN: mobile agent based detection of selfish node in MANET. Int J Wireless Mobile Networks (IJWMN) 2011, 3(4):225-235. 10.5121/ijwmn.2011.3416

[14] E. Hernandez-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A fast model for evaluating the detection of selfish nodes using a collaborative approach in manets," Wireless Personal Communications,Springer, vol. 74, no. 3, pp. 1099-1116, 2014.

[15] S. Gayathry and R. Gaur, "Handling sel_shness in manetsa survey," 2014.
[16] D.Anitha, Dr.M.Punithavalli." A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS". IJCSMC, Vol. 2, Issue. 3, March 2013, pg.112 – 119.
[17] RamasamyMurugan, ArumugamShanmugam." A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET". International Journal of Network Security, Vol.15, No.4, PP.241-247, July 2013.
[18] M. D. Serrat-Olmos, E. Hern_andez-Orallo, J.-C. Cano, C. T. Calafate, and P. Manzoni. "Collaborative watchdog to improve the detection speed of black holes in manets," 2012.
[19] ReshmaLill Mathew, Prof. P. Petchimuthu." Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs".IJARCSSE, Volume 3, Issue 3, March 2013.
[20] The network simulator - ns2. http://www.isi.edu/ nsnam/ns/