IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. V (May-Jun. 2016), PP 54-61
www.iosrjournals.org

Detection and Prevention of Selfish Attack in MANET using Dynamic Learning

Ms. Lilu Odedra[1], Prof. Ashish Revar[2], Prof. Munindra H. Lunagaria[3]
[1]*PG scholar, Department of Computer Engineering, Faculty of PG studies-MEFGI, Rajkot, India*
[2,3] *Assistant Professor, Department of Computer Engineering, Faculty of PG studies-MEFGI, Rajkot, India*

Abstract: *In this paper we deal with misbehaving nodes in mobile ad hoc networks (MANETs) that drop packets supposed to be relayed, whose purpose may be either saving their resources or launching a DoS attack. We propose a new solution to monitor, detect, and safely isolate such misbehaving nodes.in our approach watchdog method is used for observation of nodes behavior. And also varying threshold based policy is used for save nodes falsely accused in dense network. All strategies are described in detail in various paper sections with results.*

Keywords: *Network Security, MANET, Selfish attack, countermeasures, wireless security, Watchdog, threshold;*

I. Introduction

MANET is the self-organized network in which any node is free to join and leave network. In the MANET there is three types of routing protocols 1) reactive 2) proactive and 3) hybrid. The reactive protocol is on-demand protocol in this route discovery is established whenever routing is needed. This types of protocols are AODV, DSR [1] [3] etc. The proactive protocols are the table driven protocols in which each nodes route information is stored before the route discovery. Whenever the route needed the path is retrieved from routing table i.e. OLSR, DSDV [4] [2] etc. The hybrid protocol uses properties of both proactive and reactive protocols I.e. ZRP, TORA [5]. In the MANET various attacks are influence the routing due to its non-infrastructure architecture. Any unauthenticated node is join the network easily and violet the network communication. There is mainly two types of attacks are there one is the active attack and another is passive attack. In the active attack the intruder node can be unauthorized access and modified the data over the network i.e. denial of service, black hole attack, gray hole attack etc. on the other end in the passive attack the intruder node only observe the communication over the source and destination and get the important information but did not alter the data i.e. wiretapping, port scanner etc. In the MANET the mostly attacks are performed on the AODV protocol because it less secure to attacks. The attacks are the black hole, wormhole and selfish attacks which all are the type of denial of service.

This paper focus on the selfish attack and its detection and prevention technique. Selfish attack is one of the type of denials of service attack. In the network node will be act as selfish and does not forward the packets of other node towards to save its network resources for own transmission. There is many type of selfishness i.e. MAC selfish behavior, packet dropper misbehavior, partial dropping, false accusations misbehavior, set TTL field to zero misbehavior, insufficient transmission power selfishness. The reason for the node selfishness is to save own resources like energy, storage space, CPU cycles, network bandwidth etc. The node will drops all the packets of other nodes or it may use other mechanisms for saving resources. The proposed technique is uses the watchdog mechanism and the threshold based detection of selfish nodes and prevention of it. That we will see in further sections.

The rest of the paper will be organize following section (II) Related work (III) AODV protocol IV) Watchdog Technique V) Proposed Solution VI) Simulation Setups & Results VIII) Conclusion

II. Related Work

1. DREAM-Detection & Reaction to Timeout MAC layer Misbehavior

Lei Guang, Chadi Assi et al. [6] Proposed mechanism that identify the malicious nodes using a set of monitoring and reaction procedures. It use two stage reaction, first stage is for reaction and second stage is for punishment that can improve the network performance. This system gives the high accuracy in identifying misbehaved nodes. First reaction system is very effective to mitigate misbehaving effect and improve network performance.

2. LOTTO-Low Overhead Truthful Protocol for MANET

Yongwei et al. [7] proposed a scheme where a node may use dissimilar charge to send packets to different neighbors. The network topology information is collected by only one RREQ message and from that

smallest charge path from the source node to the destination node can be found. By applying VCG mechanism, LOTTO guarantee that node will get enough expense and have no incentive to cheat over their cost. It reduces overhead from O (n3) to O (n2) compared with VCG mechanism.

3. Identification of Malicious Nodes in an AODV Pure Ad Hoc Network through Guard Nodes

Imran Raza et al. [8] proposed a guard node based scheme to identify misbehaving nodes in AODV protocol. In this each node computes trust level of its neighboring nodes for route selection. Trust calculation process is based on sentiments of other nodes .The identification process of malicious nodes is dynamic due to trust level of a node is increased or decreased. If neighboring node has trust level lower than a predefined threshold, it is accusing as the malicious and does not consider in route selection.

4. A Modular Solution for Isolation

Djamel Djenouri et al. [9] proposed a solution to monitor, detect and safely isolate misbehaving nodes. The process includes five modules i.e. monitor control the forwarding of packets, Detector is to detect misbehaving of monitored nodes, isolator is used to isolate misbehaving nodes detected by detector, investigator, which investigates accusations before testifying when the node has not enough experience with accused, witness module that responds to witness request of the isolator.

5. Fighting Against Packet Dropping Misbehavior in Multi-Hop Wireless Ad Hoc Networks

Abdurrahman Baadache et al. [10] Proposed mechanism to verify the correct forwarding of packets by the intermediate nodes. The merkle tree principle is used for implementation of this approach. All intermediate nodes need to acknowledge the response of the packet. Using this source node build a merkel tree and compares the value of tree root with previously premeditated values. If both values are same then end-to-end path is packet dropper free.

6. Fully Selfish Node Detection, Deletion and Secure Replica Allocation over MANET

N.Muthumalati et al. [11] Proposed an approach which stated that Selfish node may not share its memory space to store copy for the profits of other nodes. Every node count credit risk information on other nodes individually to measure the amount of selfishness. Selfish allocation schemes reduces communication cost and secure hill cipher algorithm to provide security in replica data.

7. SENSE: A Collaborative Selfish Node Detection and Incentive Mechanism for Opportunistic Networks

Radu-Ioan Ciobanu et al. [12] Proposed an approach SENSE that offer the selfish node detection by using community based and context based information of node. By using intensive mechanism it will raise the value of the node to participate in the network. Use the unselfishness value to get the selfishness of node. It uses the home-cell community model for mobility model.

8. RTDB: Record and Trust Based Detection Technique

Senthilkumar Subramanian et al. [13] proposed a technique in which every node keeps global trust state for all nodes which is stored in trust table. The selfish nodes are detected based on their trust value and threshold for selfishness, their neighbors can use this information to avoid operation with them, either for data forwarding, data aggregation, or any other cooperative function.

9. Reputation Based Selfishness Prevention Techniques for Mobile Ad-Hoc Networks.

Alberto Rodriguez-Mayol et al. [14] Proposed a three detection techniques that improve the ability of selfishness prevention protocol to detect selfish nodes and to increase the number of valid routes. That three techniques are RAM (reset activity mode), WM (warming mode) & RFM (reset failure mode).The study of proposed techniques are implemented with TEAM & Marti's protocol.

10. TBUT (Token-Based Umpiring Technique)

Jebakumar Mohan Singh Pappaji Josh Kumar et al. [15] proposed an approach for detecting and elimination selfish nodes in MANETs using TBUT.it is the token-based umpiring technique where every node needs a token to participate in the network and the neighboring nodes acts as an umpire. Umpire nodes will monitor the behavior of the nodes and detect if any node is misbehaving. It is very efficient with reduced detection time and less overhead.

III. AODV Protocol

The Ad hoc On-demand Distance Vector (AODV) [16] routing protocol is a simple and efficient reactive routing protocol. It is designed for use in multi-hop wireless MANET. The protocol use two main

mechanisms of "Route Discovery" and "Route Maintenance", which work composed to allow nodes to discover and maintain routes to random destinations in the ad hoc network. All characteristics of the protocol operate entirely on demand.

When a node S wants to send a packet to another node D, the source node S initiates a Route Discovery by broadcasting a ROUTE REQUEST (RREQ) packet to the destination node D, which is flooded in whole the network in a controlled manner. A ROUTE REPLY (RREP) packet is unicasted to S from either the destination node D, or another middle node that knows a route to D. Every node forwarding the RREQ message stores a route back to the source node S.

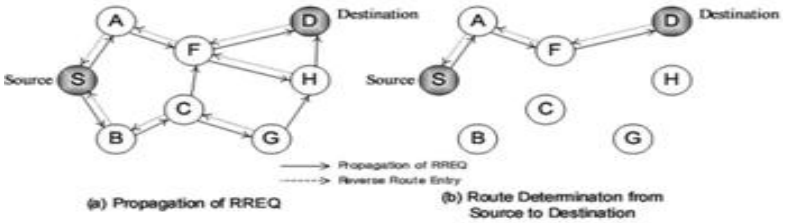

Fig 1: AODV Routing Protocol

Routes are retained by using ROUTE ERROR (RERR) message, which is sent to alert other nodes about a link breakage. HELLO messages are used by the nodes for detecting and observing links to their corresponding neighbors.

IV. Watchdog Technique

The watchdog detection technique [17] is based on the indifferent acknowledgment of the relaying of packets by at variance nodes, by overhearing the send node's transmissions, as illustrated in the example of Figure.

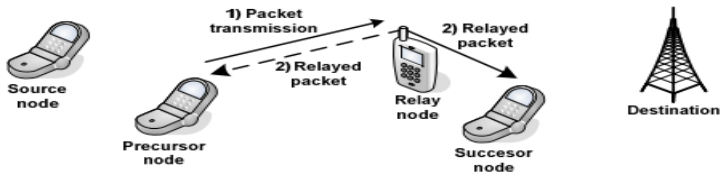

Fig 2: Watchdog Operation

In this figure, the source node has established a multi-hop connection to the destination to transmit its data packets. The route has been established subsequent a multi-hop routing protocol. The data packets are then transmitted in a hop-by-hop fashion following the sequence source node – precursor node – relay node – successor node – destination node. In Figure 2, a packet is transmitted from the precursor node to the relay node. A packets buffer in the predecessor node keeps a temporary replica of the transmitted packets that have to be forwarded by the relay node. Each buffered packet is assigned a timeout inside which the packet has to be forwarded to the successor node by the sender node. If the sender node transmits the packet within the timeout, this transmission is overheard by the precursor node, and the relay node is noted to have cooperated correctly. The precursor node looks for the copy of the packet relayed that was stored in the buffer, and removes the copy. If the relayed packet is not overheard correctly by the precursor node within the timeout, then the relay node is assumed to have acted selfishly, i.e. it has dropped the packet. This is referred to as selfish behavior detection. Some countermeasures are taken, depending on the SPP considered, affecting the trust level of the relay node in the reputation table of the precursor node. An important parameter of the watchdog detection process is the packet timeout, which refers to the time within which the relay node must relay the packet

V. Proposed Technique

Figure 3 shows the conceptual architecture of proposed architecture of detection and prevention of selfish attack.in this various modules are used for the different purpose. And the process is executed from top to bottom step wise.

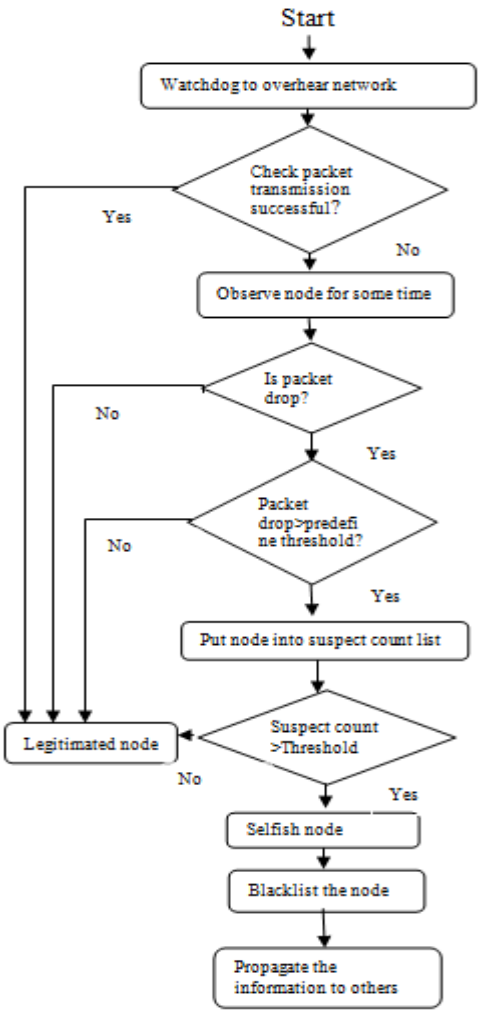

Fig 3: Proposed Framework

The Proposed framework is shown in the Fig-3 in this the watchdog method is used to observe the neighbor nodes activity. Then check that transmission of the packet is successful or not by observe the acknowledgment of received nodes. If transmission is successful then continue the routing process and if transmission is not successful than observe that node for some time and if it continues to drop packets than consider as suspected node.it checks then packet drop greater than predefine threshold value or not. If packet drop greater than threshold then node is suspected as selfish node and added to the suspect count list. If suspect count of that node greater than the threshold then node declare as a selfish and blacklisted from the network. Then after all information about that node is propagated in the network.

VI. Simulation Setups & Results

The simulation was done using the NS-2. Simulator [18], which provides a salable simulation environment for wireless networks. In order to measure the impact of selfish nodes in ad hoc network performances, the AODV implementation was modified using the NS-2 simulator. Table I represents the simulation parameters along with their corresponding values. The simulated network consists of 25,50,75,100 nodes placed randomly in 500x500 areas and we are performing two evaluation scenarios 1) one selfish node and varying number of nodes 2) static number of nodes i.e 25 and varying selfish nodes i.e. 2,4,6,8. Each node moves at a speed of 4.0 m/s.

The CBR file and Scenario is generated with following commands in ns 2.35.

- ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] –seed seed] [-mc connections] [-rate rate] > cbr_filename
- ./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] [-X maxx] [-Y maxx] > scen_filename

1. Varying Number Of Nodes

In this scenario we are taking varying number of nodes in the network and show effect of network at one selfish node in the network.

TABLE- I Simulation Parameters scenario 1

Parameter	Value
Simulator	NS-2.35
Protocol	AODV
Simulation Time	100s
No of Mobile Nodes	25,50,75,100
Area	500x500
Traffic Type	CBR
No of Selfish Nodes	1
No of. Connections	10
Threshold value	10

1. Throughput

Throughput or network throughput is the average rate of successful message delivery over a network. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

As shown in the Figure 4, for various no. of nodes the throughput is decreased as selfish node is present in network. The selfish nodes drop the routing packets of other nodes and the average throughput of the network is decrease. We can show in the figure that proposed scheme improve the network Throughput with selfish node present in the network.

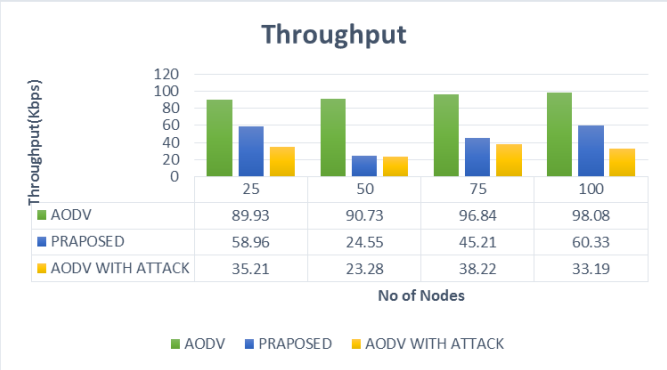

Fig 4: Varying number of nodes vs. 1 selfish node

2. Packet Delivery Ratio

It is the percentage of total number of packets received by the intended receivers to the total number of packets originated by all nodes.

As shown in the Figure 5, the packet delivery ratio of network is decreased as presence of selfish node in network while as shown in graph proposed scheme improve the packet delivery ratio by identifying selfish nodes and remove it from network and gives the better results as compare to presence of selfish nodes in the network.

3. Goodput

Goodput is the average rate of successful data packets delivery over a network.it only consider data packets and it is the ratio of forwarded packets without control packets. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

As shown in the Figure 6, the packet Good put of network is decreased as selfish node Presence in the network .it is network throughput without the control packets, its only consist data packets. Compare to absence of selfish nodes, when there is a presence of selfish nodes the Goodput is decreased and network performance is degraded.the proposed technique gives the better improvement in results as we can see in the graph.

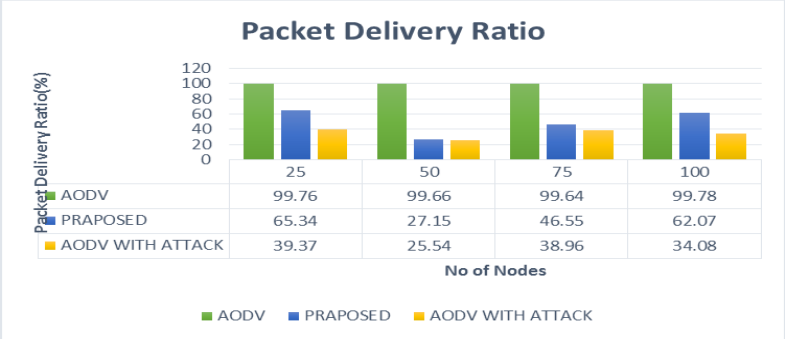

Fig 5: Varying Number of Nodes Vs. 1 Selfish Node

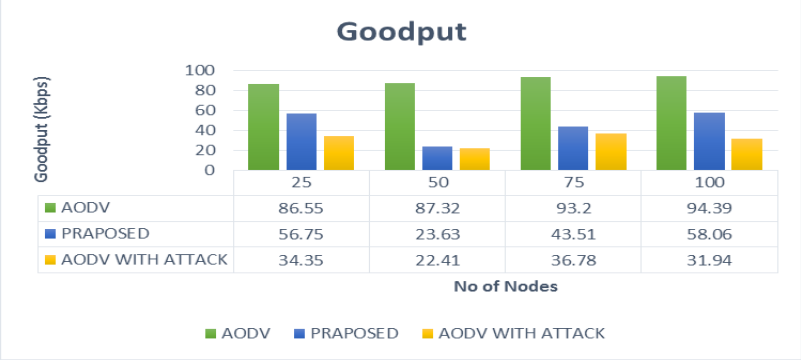

Fig 6: Varying Number of Nodes vs. 1 Selfish Node

2. Varying Number of Selfish Nodes

In this scenario we are taking static number of nodes in the network and show effect of network at varying selfish node in the network.

TABLE- II Simulation Parameters scenario 2

Parameter	Value
Simulator	NS-2.35
Protocol	AODV
Simulation Time	100s
No of Mobile Nodes	25
Area	500x500
Traffic Type	CBR
No of Selfish Nodes	2,4,6,8
No of. Connections	10
Threshold	10

1. Throughput

As shown in the Figure 7, with the increase the number of selfish nodes in the network the throughput of the decrease continuously.as shown in graph the proposed scheme improve the performance under the varying selfish nodes and increase the throughput

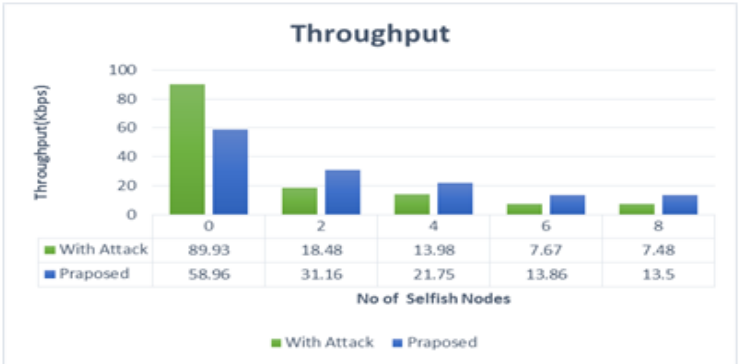

Fig 7: 25 Numbers of Nodes vs. Varying Selfish Nodes

2. Packet Delivery Ratio

As shown in the Figure 8, the packet delivery ratio of network is decreased as the number of selfish nodes increase in network while as shown in graph proposed scheme improve the packet delivery ratio by identifying selfish nodes and remove it from network.

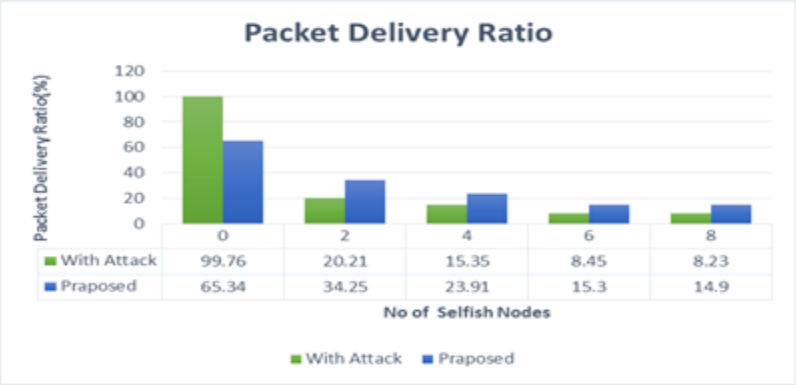

Fig 8: 25 Numbers of Nodes vs. Varying Selfish Nodes

4. Goodput

As shown in the Figure 9, the packet Good put of network is decreased as selfish nodes increase in the network .it is network throughput without the control packets, its only consist data packets. Compare to absence of selfish nodes, when there is a presence of selfish nodes the Goodput is decreased and also results shows that when use the proposed scheme the good put is increased as compare to results with presence of selfish node in network.

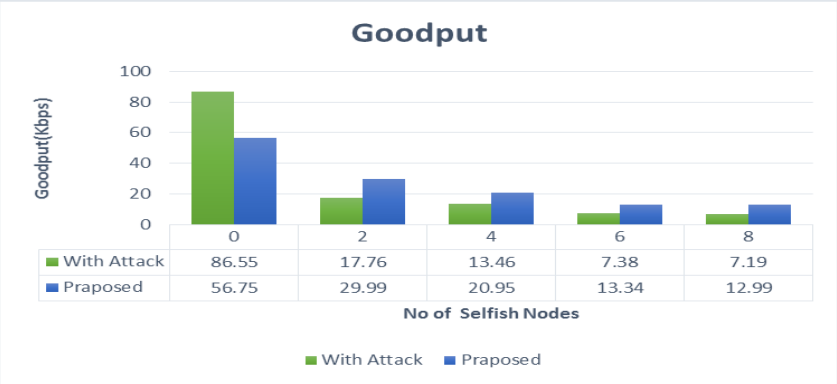

Fig 9: 25 Numbers of Nodes vs. Varying Selfish Nodes

VII. Conclusion

In this paper, the simulation of AODV Protocol under without selfish attack and with selfish attack and with proposed scheme has been carried out using NS-2.35 simulator. Simulation has been done for two scenarios1) 25 nodes in ad hoc network and 0(no selfish nodes), 2, 4, 6 and 8 selfish nodes and 2) 25, 50, 75 and 100 nodes in network and one selfish node. It has been analyzed both protocols in terms of throughput, Packet Delivery Ratio and Goodput. If we include concept of selfish behavior node in AODV protocol then in enhanced version of protocol, the results of simulation show that this has far above the ground effect on AODV protocol. From the simulation results and as shown in graphs that if we include selfish behavior node in AODV protocol then there is significant decrement Throughput which indicates selfish nodes drops the packets and it will result in network degradation. Packet delivery ratio is decreased as increase in no. of selfish nodes. Goodput is decreased as increase in no. of selfish attack. The proposed scheme which uses the concept of watchdog observation and threshold base scheme for improve the network performance, as shown in results of both the scenario the proposed scheme is provide significant improvement of network performance and reduce the effect of selfish nodes. The drawback of this scheme is that it cannot detect the collaborative attacks and also it use watchdog mechanism so it will fail to detect the selfish nodes if they working collaboratively. Another drawback is the isolated node in never able take part in routing after it isolated. Future work is to improve this scheme by overcoming its drawback and improve the performance by using some other new mechanism which detect collaborative attacks and mechanism by which node can take part in routing after some time after it isolated from network.

References

[1] Shao, Baohua. "Performance of Ad Hoc on Demand Distance Vector Routing Protocol." *In 2010 International Conference of Information Science and Management Engineering*, pp. 420-421. IEEE, 2010.

[2] Mahdipour, Ebrahim, Amir Masoud Rahmani, and Ehsan Aminian. "Performance evaluation of destination-sequenced distance-vector (dsdv) routing protocol." *In Future Networks, 2009 International Conference* on, pp. 186-190. IEEE, 2009.

[3] J. Broch. D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," *IETF Internet draft, draft-ietf- manet-dsr-01 txt, Dec. 1998*

[4] Hilippe Jacquet, Paul Muhlethaler, Amir Qayyum, Anis Laouiti, Laurent Viennot and Thomas Heide Clausen "Optimized Link-State Routing Protocol", draft-ieft-ols r-04.txt - March 2001

[5] A.vani." Study of MANET Routing Protocols TORA, LDR, ZRP." *International Research Journal of Engineering and Technology (IRJET)* on, pp. 1889-1891. vol-2,issue-3(2015).

[6] Guang, Lei, Chadi Assi, and Yinghua Ye. "DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks." *Computer communications* 30, no. 8 (2007): 1841-1853.

[7] Wang, Yongwei, and Mukesh Singhal. "On improving the efficiency of truthful routing in MANETs with selfish nodes." *Pervasive and Mobile Computing* 3, no. 5 (2007): 537-559.

[8] Raza, Imran, and Syed Asad Hussain. "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes." *Computer Communications* 31, no. 9 (2008): 1796-1802.

[9] Djenouri, Djamel, and Nadjib Badache. "On eliminating packet droppers in MANET: A modular solution." *Ad Hoc Networks* 7, no. 6 (2009): 1243-1258.

[10] Baadache, Abderrahmane, and Ali Belmehdi. "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks." *Journal of Network and Computer Applications* 35, no. 3 (2012): 1130-1139.

[11] Muthumalathi, N., and M. Mohamed Raseen. "Fully selfish node detection, deletion and secure replica allocation over MANET." In *Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on*, pp. 413-415. IEEE, 2013.

[12] Ciobanu, Radu-Ioan, Ciprian Dobre, Mihai Dascălu, Ştefan Trăuşan-Matu, and Valentin Cristea. "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks." *Journal of Network and Computer Applications* 41 (2014): 240-249.

[13] Subramaniyan, Senthilkumar, William Johnson, and Karthikeyan Subramaniyan. "A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique." *EURASIP Journal on Wireless Communications and Networking* 2014, no. 1 (2014): 1-10.

[14] Rodriguez-Mayol, Alberto, and Javier Gozalvez. "Reputation based selfishness prevention techniques for mobile ad-hoc networks." *Telecommunication Systems* 57, no. 2 (2014): 181-195.

[15] Kumar, Jebakumar MSP Josh, 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, no. 1 (2015): 143.

[16] Rodriguez-Mayol, Alberto, and Javier Gozalvez. "Improving selfishness detection in reputation protocols for cooperative mobile ad-hoc networks." In *Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on*, pp. 2533-2538. IEEE, 2010.

[17] Mubashir Husain Rehmani,Sidney Doria, and Mustapha Reda Senouci " A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)" June 2009