An Efficient and Secure Algorithm to Eliminate the Routing Misbehavior In MANETs

N Priyanka, Bhagirathi N M

Abstract— One of the emerging technologies in wireless communication is Mobile Ad Hoc Networks. A Mobile Ad Hoc Network(MANET) is a collection of mobile nodes which communicate with each other via wireless links either directly or relying on other nodes such as routers. These networks can be set up easily anywhere and anytime without any base infrastructure, thus proving to be very efficient in various applications such as military environments, emergency operations, collaborative and distributed computing, wireless sensor networks, personal area networks etc. The cooperativeness between the nodes is vital for the communication among the nodes. But in open MANETs, some nodes deviate from the normal behavior thus causing misbehavior in the network. The misbehavior is caused by selfish nodes which refuse to forward the data packets for other nodes in order to conserve their own energy. Securing the MANETs in an untrustworthy environment is always a challenging problem. This paper implements an efficient and secure algorithm to eliminate the misbehavior and evaluates the performance of the network in terms of throughput, average end to end delay and packet delivery ratio.

Index Terms— AODV, Cryptography, Misbehavior, MANET, Registration node, Selfish nodes, 2ACK scheme.

1 INTRODUCTION

Mobile Ad Hoc Network is a self configuring, infrastructureless network of moile devices communicating with each other via wireless links either directly or relaying on other nodes as routers. Network nodes are free to move randomly. The network topology changes randomy and unpredictably. All network functions such as routing, multihop, packet delivery and mobility management hve to be performed by the member nodes themselves, either individually or collectively. Communication between two nodes is established only if the Euclidean distance between them is less than the transmitting range. Fig 1 shows the Typical structure of MANETs.

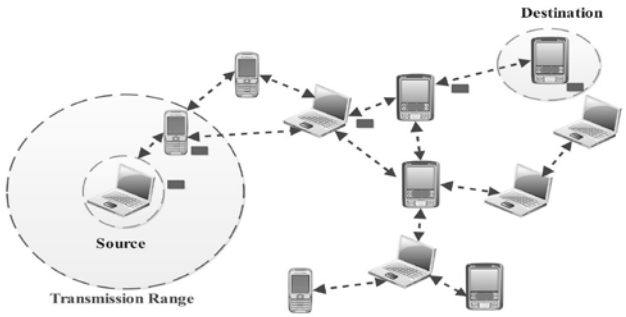

Figure 1: Typical structure of MANETs

There are two types of MANETs: closed and open. In a closed MANET, all the nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be the most important resource in a mobile environment.

Open environment of a MANET may lead to misbehaving nodes. Such nodes are also called as selfish nodes and the behavior is called routing misbehavior as they cause malfunctioning in the normal working of a routing protocol. Misbehaving nodes come into existence in a network due to several reasons :

1. Mobile hosts lack adequate physical protection due to the open communication medium i.e., any number of nodes can join and leave the network anytime.
2. Usually mobile nodes are resource constrained computing devices.

A selfish node may refuse to relay a packet aiming to economize its energetic resources in order to extend its life time or simply because its battery power is drained.

There are three misbehaving node models :

1. Selfish node of type 1 (SN1): An SN1 node does not perform any packet forwarding function for the data packets unrelated to itself. However it operates normally in the Route Discovery and the Route Maintenance phases of the protocol.

2. Selfish node of type 2 (SN2): An SN2 node neither participates in the Route Discovery/Maintenance phase nor in the data packet forwarding. It only spends its battery energy to send or receive its own data packets.

3. Selfish node of type 3 (SN3): An SN3 node 's behavior depends on the energy levels of the nodes. When the energy lies between full energy E and a threshold T1, the node behaves properly .For an energy level between T1 and another lower Threshold T2, it behaves like a node of type SN1.Finally, for an energy level lower than T2, it behaves like a node of type SN2. The relationship between T1,T2 and E is T2< T1<E.

There are various types of attacks which arises due to the presence of misbehaving nodes in the network. One such attack is a Black hole attack against network integrity absorbing all data packets in the network. Black hole attack is one of the security issues in MANET. In this attack, the malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Once intercepted, malicious node attracts the packets towards it and discard (or drop) the packets without informing the source that the data did not reach its intended recipient. Fig 2 depicts MANET with misbehaving nodes.

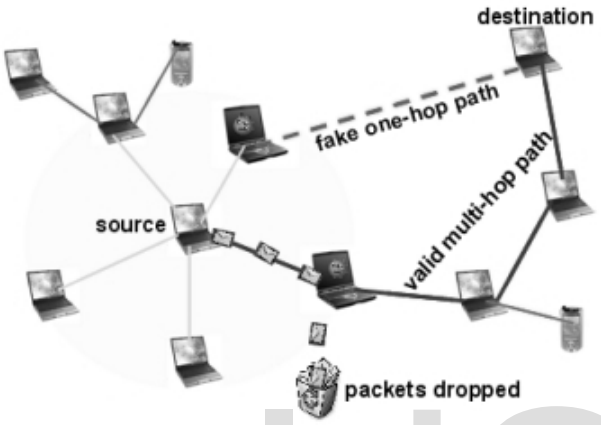

Figure 2: MANET showing misbehavior

This paper focuses on the prevention of Black hole attack by eliminating the selfish nodes particularly selfish nodes of type 1(SN1) thus increasing security in the network.

2 Literature Review

Various techniques have been implemented to eliminate the selfish nodes. These techniques can be divided into the following categories:

1. ***Credit based schemes:*** In credit based schemes also called incentive based schemes, the goal is to provide incentives for nodes to faithfully perform networking functions. Nodes get paid for providing services to other nodes. These schemes are implemented using two models: Packet purse model and Packet trade model.

This scheme has the disadvantage that they are not scalable due to the central virtual bank. Some kind of temper-resistant hardware and extra protection for the payment system or virtual currency is required as it requires some kind of incentive transaction.

2. ***Reputation based schemes:*** In these schemes, the nodes collectively detect and declare the misbehavior of a suspicious node. Declaration is propagated throughout the network so that the misbehaving nodes will be cut off from the rest of the network. These schemes do not need any centralized entity as in the credit based schemes. There are two models: Watchdog and Path rater.

The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overhead packet with the packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

The path rater, run by each node in the network, combines knowledge of misbehaving nodes with the link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. If there are multiple paths to the same destination, the path with the highest metric is chosen.

Nodes suspected of misbehaving by the watchdog mechanism are assigned a special highly negative value. When the path rater calculates the path metric, negative path value indicate the existence of one or more suspected misbehaving nodes in the path. If a node were marked as misbehaving due to a temporary malfunction or incorrect accusation it would be preferable if it were not permanently excluded from routing. Therefore nodes that have negative ratings should have their ratings slowly increased or set back to a non-negative value after a long timeout.

In watchdog and path rater methods, wireless interfaces that support promiscuous mode operation are assumed, which is not appropriate for all the mobile ad hoc network scenarios. Also, the watchdog technique has the weaknesses that it might not detect a misbehaving node in the presence of: Ambiguous collision, Receiver collisions, Limited transmission power, False misbehavior, Collusion and Partial dropping.

3. ***End-to-End Acknowledgement based schemes***: In this scheme, acknowledgements are sent by end receiver to the sender to inform it that the packets have been received successfully up to some locations of continuous data stream. These schemes adds to routing overhead in the network but increases reliability and throughput of the network.

Some of the existing acknowledgement schemes are described as follows:

i. *1-ACK Scheme:* This scheme is based on single or 1-hop acknowledgement packet that is sent by receiver to sender. When node forwards data packet to the next node in the routing path, the receiving node will send back the acknowledgement called ACK which indicates that data packet has been received successfully. This scheme overcomes problems which occur in reputation based schemes. But routing overhead in-

creases in this scheme.

ii. *SACK (Selective Acknowledgement) Scheme*: In this scheme, acknowledgement packet will be sent for certain amount of data packets received from same source node thus reducing the routing overhead substantially compared to that in 1-ACK scheme.

iii. *TWOACK scheme:* It detects the misbehaving link by acknowledging every data packet transmitted over each three consecutive nodes along the path from source to destination. Packet TWACK is sent back two hops for every data packet received thus increasing reliability as well as network overhead. If the source node does not receive a TWOACK acknowledgement packet for data packet sent, the next hop's forwarding link is claimed to be misbehaving.

This scheme fails to detect malicious nodes in the presence of false misbehavior report and forged ACK packets as the source node immediately trusts the misbehavior report provided by other nodes.

iv. *Selective TWOACK (S-TWOACK) scheme*: It is a derivative of TWOACK scheme with almost the same performance without any routing overhead but with some expected increase of false alarms.

v. *AACK (Adaptive Acknowledgement) scheme:* It is a combination of TWOACK and end-to-end acknowledgement scheme ACK. As compared to TWOACK, this method significantly reduces network overhead while maintaining the network throughput. But it fails to detect malicious nodes in the presence of false misbehavior report and forged acknowledgement packets.

All the above mentioned schemes for the detection and elimination of misbehavior in the network suffer from some or the other disadvantages.

3 AODV Routing Protocol

AODV is one among the reactive routing protocols used in MANETs. The route is generated at the start of the communication. Each node has its own sequence numbers which increases whenever changes in the link occur. The freshness of the channel information is based on the sequence numbers. AODV uses Open path shortest first (OSPF) method which is based on Dijkstra's algorithm for finding the shortest path between source and destination. It is well suited for the dynamic topology such as MANETs as it handles any changes in the routes and finds new routes whenever there is an error.

AODV includes 4 different control messages. They are as follows:
i. Route Request(RREQ) : In route request, the source node transmits or broadcasts the route request message for specific destination and the neighbor nodes which do not have the path to the destination forwards the message to the intended recipient.
ii. Route Reply (RREP) : In route reply, the destination unicasts the reply message to source, neighbor nodes make next hop node entry for destination and forwards the reply. If the source receives multiple replies at the same time, it uses the path with the shortest hop count.
iii. Route Error(RERR): Route error message is generated in the network whenever a link breaks between source and destination. The broken route is assigned an infinite hop count and a sequence number increased by one. AODV detects the node and if possible does the local repair.
iv. HELLO messages: Hello message always supplies the route to itself i.e., the hop count field is set to zero. A node keeps track of its neighbors by listening for the HELLO messages that each node broadcasts at set intervals.

AODV is vulnerable to various kinds of attacks because it is based on the assumption that all nodes will cooperate. Without this cooperation, no route can be established and no packet can be forwarded.

4 Algorithms Involved

In this paper, selfish node behavior is implemented on AODV routing protocol and the behavior is analyzed by measuring the network performance in terms of throughput, packet delivery ratio and average end to end delay. Then the algorithms which are involved in detecting and eliminating the misbehavior are implemented and the network performance analyzed. The algorithms are explained below.

4.1. Node Registration

It is a secure cryptographic algorithm to eliminate the misbehavior in MANETs. In this algorithm, a registration node is created which acts as the admin of the network which configures the nodes to allow access. A token is generated and distributed to the nodes when a request is made. This token is valid only for a certain duration.

The technique consists of the following steps:

i. A dedicated node called registration node(RN) is created whose function is to generate and assign registration tokens to each and every node.

ii. The nodes request to RN for registration token when they have to communicate with each other.

iii. The request packet contains source node identity, timestamp, home address and token request.

iv. The RN checks the node identity and its home address to identify to which network it belongs to.

v. After successful confirmation, RN generates a registration token and assigns it to the requesting node. Registration token contains node ID, timestamp, duration, public key, nonce and that token is encrypted using private key of RN.

vi. The source sends an ACK signal to RN after it receives the registration token. The ACK signal contains node ID, timestamp and nonce and will be encrypted using public key of RN.

vii. Steps iii-vi will be carried out between the destination and RN too.

viii. After the source and the destination receives the registration token, the communication begins.

This technique ensures that only valid and authentic nodes only communicate thus eliminating the invalid i.e., the selfish nodes in the network. It also reduces the number of messages among the nodes, reduces delay in registration of different nodes and reduces bandwidth consumption.

4.2. 2ACK Algorithm

It is one among the end-to-end acknowledgement schemes to detect the misbehaving link in the network. It overcomes the weaknesses of the previous algorithms. In the approach, only a fraction of the data packets are acknowledged thereby reducing the overhead. Fig 3 shows the working of 2ACK scheme.

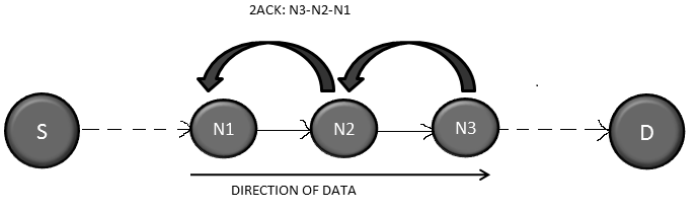

Figure 3: Working of 2ACK scheme

Consider a two hop path of N1-N2-N3 where N1 is the source and N3 is the destination. Each node consists of a client and a server and the function of the server is to forward the data packets it receives from the same node's client to the next hop on the path. When N1 wants to send a message to N3, the client of N1 forwards the message to the server of N1 which then forwards the message to the client of N2. Simultaneously N1 also starts a timer. The process continues till message reaches client of N3. After receiving the message the node N3 sends a 2ACK packet to N1. The function of N2 is to forward the packet to N1. On receiving the 2ACK packet N1 checks the status of the timer started for the packet sent to N3. If N1 receives the packet from N3 after expiry of the timer or if it does not receive the packet at all then it will report node N3 as a malicious node. The triplet N1-N2-N3 is used for reducing the network complexity and time. If we take more number of hops then it will take more time. So we just consider the triplet for detecting misbehavior in MANETs. In case of misbehavior server doesn't forward the 2ACK packet to the next hop's client. When N1's client does not receive a 2ACK packet, it increments parameter Cmis which keeps a count of the number of 2ACK packets missed. At the end of the process ratio Cmis/Cpkts is calculated where Cpkts is the count of the forwarded data packets. If the value is greater than Rmiss i.e., the threshold to determine the allowable ratio of the total number of 2ACK packets missed to the total number of data packets sent, then the link is considered to be misbehaving and the information is displayed at the source node.

5 Simulation Scenario

The simulation contains 20 nodes scattered on a 730×700 meter flat space for data transfer. The physical layer and 802.11 MAC layer are included. Table 1 shows the other simulation parameters. TCP with constant bit rate (CBR) traffic is used with packet size of 512 bytes. The routing protocol used is AODV routing protocol which is a reactive routing protocol i.e., it creates the routes when demanded by the source. Two selfish nodes are introduced into the network to misbehave the network. The simulation parameters is shown below.

Table 1: Simulation parameters

PARAMETERS	VALUE
ROUTING PROTOCOL	AODV
SIMULATOR	NS 2.35
TOPOLOGY	730*700
NO OF NODES	20
SIMULATION TIME	40 sec
NO OF SELFISH NODES	2
PACKET SIZE	512 bytes
ENERGY OF NODES	5 joules
ENERGY MODEL	EnergyModel
RADIO PROPAGATION MODEL	TwoRayGround

In this paper, the energy of the nodes is considered. The energy model represents the energy level of a node. The nodes are assigned the initial value of energy as 5 joules. The energy of a node decreases as and when an event occurs. The events are: transmitting a packet, receiving a packet, energy consumption in idle state, energy consumption in sleep state and transition from sleep state to active state. Receiving and transmitting

packets are the major events that consumes most of the node's energy.

The radio propagation model used is two ray ground model which considers both the direct path and a ground reflected path. the model gives more accurate prediction at a long distance than the free space model.

In this paper, the behavior of the MANET with and without the misbehavior are compared and the methods i.e., the node registration and 2ACK scheme are applied into the misbehaving network. Then the performance of the network is analyzed by measuring the parameters : Throughput, packet delivery ratio and average end-to-end delay.

6 Performance Metrics

1. ***Throughput:*** It is defined as the average rate of successful message delivery over a communication channel.

2. ***Packet delivery ratio:*** It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

3. ***Average end-to-end delay:*** The average time taken for a packet to be transmitted across the network from source to destination. It includes the delays due to route discovery, queuing, propagation delay and transfer time.

7 Results And Conclusion

The following Fig 4 shows the network with 20 nodes among which two are selfish nodes shown in red. These selfish nodes attracts the packets without informing the source that the data did not reach its intended recipient. They use the routing protocol to advertise themselves as having the shortest path to the destination.

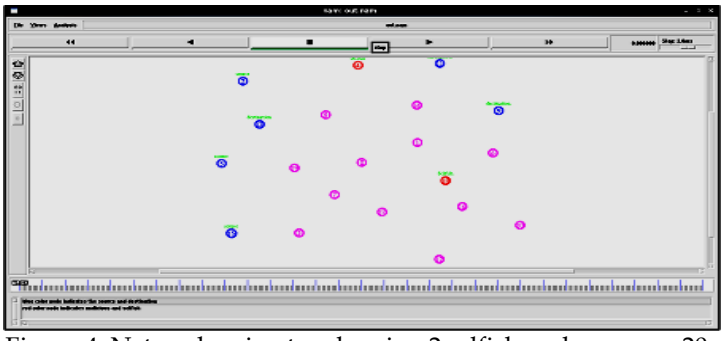

Figure 4: Network animator showing 2 selfish nodes among 20 nodes

Fig 5 shows the network with the registration node and 2ACK scheme.

Fig 6,7 and 8 shows the graphs of packet delivery ratio, throughput and average end-to-end delay, vs. simulation time

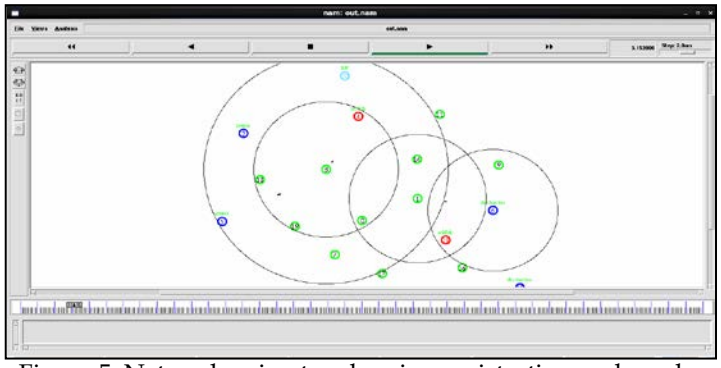

Figure 5: Network animator showing registration node and 2ACK

respectively compared for the normal network, network with misbehavior and the network with 2ACK+AODV and registration node. It is observed that the misbehavior in the network decreases the performance of the network. Therefore, the methods implemented for eliminating the misbehavior increases the performance of the network.

The average end-to-end delay for the network with 2ACK+AODV and registration node is increased compared to the normal network due to the 2ACK scheme and registration node employed. The packet delivery ratio reaches the value nearer to the value obtained for the normal network. The throughput is increased compared to the normal network.

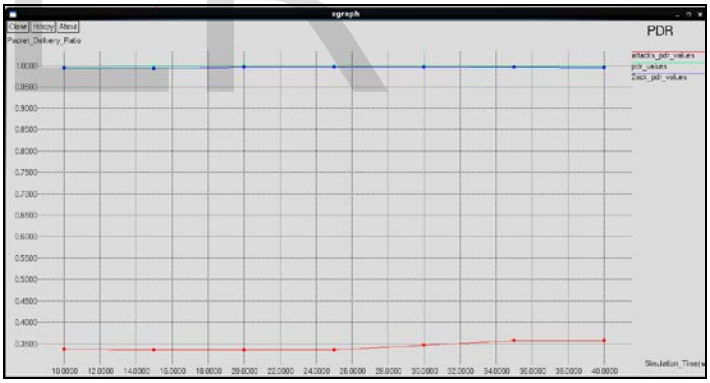

Figure 6: Xgraph for packet delivery ratio vs. simulation time

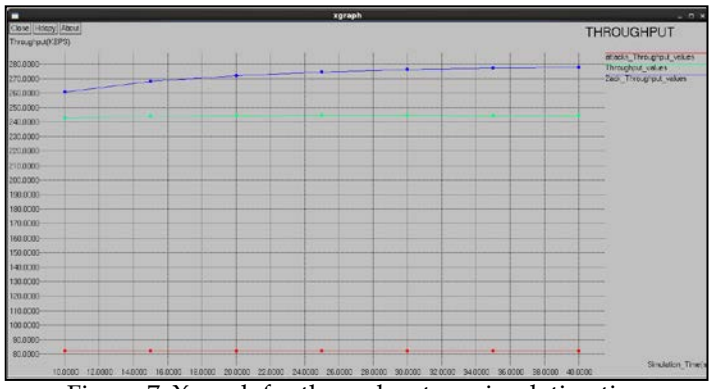

Figure 7: Xgraph for throughput vs. simulation time

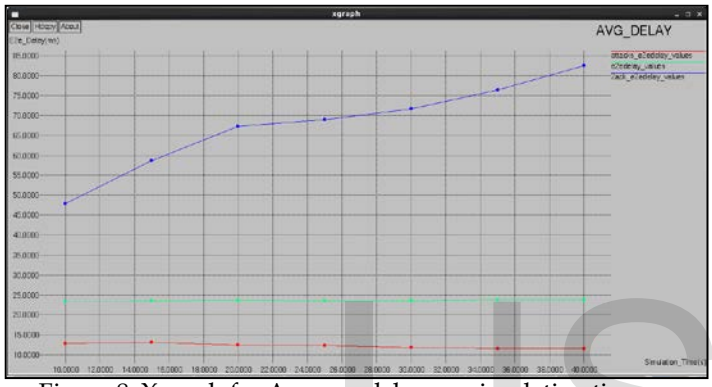

Figure 8: Xgraph for Average delay vs. simulation time

based Adhoc Wireless Networks", International Journal of Computer Engineering And Technology (IJCET), ISSN: 0976-6367, Volume 5, January 2014.

[2] Mrunal Pathak, Jyoti Hotte, "Survey on Acknowledgement Based Schemes For Misbehavior Detection in Manet", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-4, April-2014.

[3] Prof. Ravindra Rathod, Prof M. D. Ingle, Prof. Bharat S Kankate, Prof R. M. Kawale, "Detection of Routing Misbehaving Links in MANET by 2ACK Scheme", International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 2, February 2013.

[4] Nada M. Badr and Noureldien A. Noureldien, "Review of mobile ad hoc networks security attacks and countermeasures", International journal of computer engineering & Technology 2013.

[5] Namrata Marium Chacko, Getzi P. Leelaipushpam, "A Reactive Protocol For Privacy Preserving Using Location Based Routing In Manets", IJCSN International Journal of Computer Science and Network, Vol 2, Issue 2, April 2013.

[6] Sonali Gaikwad and Dr. D. S. Ada , "Reduction in routing overhead in MANET using 2-ACK scheme and Novel routing Algorithm", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013.

[7] Gaurav Soni and Kamlesh Chandrawanshi, "A novel defence scheme against Selfish Node Attack in Manet", International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, June 2013.

[8] Manoj V. Mori1, G.B. Jethava, "Node registration in MANET", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 1, January - February 2013.

[9] Aravindh S, Vinoth R S and Vijayan R, "A Trust Based Approach for Detection and Isolation of Malicious Nodes in Manet", International Journal of Engineering and Technology (IJET) Vol 5 No 1 Feb-Mar 2013.

[10] Prof. Shalini V. Wankhade," 2ACK-Scheme: Routing Misbehavior Detection in MANETs Using OLSR", July 2012.

[11] Isha V. Hatware, Atul B. Kathole, Mahesh D. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.

[12] Chinmaya Kumar Nayak, G K Abani Kumar Dash, Kharabela parida and Satyabrata Das, "Detection of Routing Misbehavior in MANETs with 2ACK scheme", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.1, January 2011.

• *Ms. N Priyanka is currently pursuing masters degree program in Digital Electronics and Communication in Bangalore Institute Of Technology, Karnataka, India.*
• *Smt. Bhagirathi N M is currently Assistant Professor with 24 years of teaching experience in Digital Switching Systems, Computer Networking, Wireless Communication in Bangalore Institute Of Technology, Karnataka, India.*

REFERENCES