International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-03, Issue-3 E-ISSN: 2347-2693

Preventing Packet Dropping Attack in Ad hoc Networks Using Malicious node Isolation Model

S.Madhurikkha[1*], C. Meenu Kumari[2],S.Revathi[3] and P.Nathiya[4]

[1,2,3,4]*Department of Computer Science, Jeppiaar Engineering College, India*

www.ijcseonline.org

Received: Feb/24/2015 Revised: Mar/06/2015 Accepted: Mar/22/2015 Published: Mar/31/2015

***Abstract*—**Securing ad hoc network is one of the trending issues that is going on in the networking industry which has lead to the development of various algorithms and methods for identifying intrusions. Intrusions are of various types namely packet forwarding attack, black hole, sequence numbers etc., there are still so many such intrusions that are taking place. The proposed project is to study the impact of a malicious node in the ad hoc network. The proposed system uses MNI-AODV algorithm by using malicious node isolation(MNI) method. In this paper methods against malicious node is implemented by introducing MNI-AODV in the ad hoc network [7]. The impact of nodes in the presence of packet dropping attack is also presented.

***Keywords*—** *Network Security, Malign nodes, ad hoc and network attacks, ns2.*

I.INTRODUCTION

Numerous algorithms have been proposed for detecting the interventions in the networks. These interventions are due to the presence of malicious nodes. Detecting or identifying the malicious node is presented in the works that are already done[1-5]. The paper focus on way on isolating the malign node using the MNI-AODV algorithm. Hence, the performance of the entire network can be improved.

There are many mysterious routing protocols projected till now. We use thetopology-based type of on-demand mysterious routing protocols, which are common for MANETs in a different environments. If we develop the anonymous protocols, a direct method have to anonymize the mostly used on-demand ad hoc routing protocols, like AODV and DSR. For this reason, among the source,destination and the node we have to estimate the anonymous security associations. The resulting protocols like ANODR, SDAR, A non DSR, MASK and Discount-ANODR. After evaluating these protocols, we find that the objectives of unindentifiability and unlink ability are not fully satisfied. For example, ANODR focuses on protecting the node or route identities during a route discovery process, especially on the routing packets, e.g., Route REQuest (RREQ) and Route REPly (RREP). ANODR uses the message from RREQ, rather than using the ID of the destination node. However, the route can be identified by RREQ message, which may be on the rampage to the intermediate nodes in backward RREP forwarding. The other protocols rely on the neighborhood detection and authentication, but may partially violate the anonymity requirements for performance measures. For instance, in SDAR, the node and its individual hop neighbors are made to know each other's ID during the routing procedures. In MASK and Discount-ANODR, a clear node ID is used in the route discovery.

II.RELATED WORKS

A list of works that has been done to ensure the security in the ad hoc network is listed below:

In [9], Jaydipsen et al, worked on a cooperative scheme which could detect the malign nodes, where every node monitors the neighbouring nodes behaviour. The attack in the network was found using the Distribution Algorithm, as routing was secured using trusted nodes only, it is an overhead and malicious nodes are not isolated in this method.

In [8], Muhammad et al, worked on a two folded solution which both detected and identified the malign nodes using Tmax (maximum threshold) and monitoring nodes to
declare misbehaving nodes. But it failed to detect and isolate the attackers in the group network.

In [11], Marti et al, proposed a mechanism watchdog and path rather identifies the malign nodes. Promiscuous mode of operation was used in this scheme. Misbehaviours in presence of ambiguous collision, limited transmission power, false misbehaviours and partial dropping it lacks deficiency would be failed by using watchdog method.

In [10], Sirisha et al, proposed a method where a malicious nodes that drop packets in MANET by setting rules for nodes with low false positive rateare detected by a manager. The misrouting behaviour of the node in networkcannot be detected by the detection manager.

In [12], Bhalaji.N et al, proposed enhanced security for selective packet drop attack usin an association based routing using DSR protocol which is based on trust value and threshold parameters between nodes. But the cost of maintaining the association table for each node is not evaluated.

III.OVERVIEW OF AODV ROUTING PROTOCOL

Ad hoc On Demand Distance Vector(AODV) is a descendent of Destination Sequenced Distance Vector (DSDV) routing protocol. It establish the route from source to destination only on demand. Each Nodes has a routing table that says about the next hops. loop-free routing and count-to-infinity problem are avoided inAODV by using destination sequence number in routing table. It tells the freshness of the route to destination. The source nodefirst checks its own routing table to determine whether a route to destination is already availablewhen it wants to route packets to destination node. If yes the packet is routed to the destination. If not, the source nodebroadcasts a route request (RREQ) message to its neighbours which is further propagated until it reaches an intermediate node with fresh route to destination node or destination node itself by initiating a route discovery process. The intermediate nodes on receiving RREQ make an entry in their routing table for the node and source node. The node relays a further request to its neighbours, if the destination sequence number present in routing table is lesser than or equal to number present in RREQ packet. If the Sequence number is higher, it denotes a "fresh route" and packets can be sent through this route. The intermediate node or the destination node with fresh route to destination unicasts route reply (RREP) message to neighbouring nodes from which it received RREQ.

IV. FLOODING ATTACK

Provision of security to nodes in the MANET is a tedious job. Flooding is a type of Denial of Service (DoS) attack in MANET. Disturbance in the network operation will be caused due to the flooding. This kind of attack consumes battery power, storage space and bandwidth. The performance of the network will be degraded by flooding excessive number of packets in the network. Here a hello flooding packets are used. The neighbour node does not process the other nodes as the hello flooding packets are sent continuously. If the hello packet is not found then it will lead to a wrong assumption that the neighbouring node has moved away.Meanwhile one of the intermediate node sends a ERR to the source to reinitiate the path. This study identifies and prevents the flooding attack. Packet delivery ratio, delay and throughput are the performance parameters used in this. This algorithm is implemented in Secure AODV and tested in ad hoc environment.

The Fig.1 represents the architecture diagram of the proposed system. In this construction of 'n' nodes are did first. Once the nodes are constructed, source will check the routing table for finding the path to send the data from source to the destination. After checking the routing table, RREQ is broadcasted to the intermediate nodes.If the intermediate node finds an error in sending the data,it would immediately send the error message to the neighbouring node.Since the error messages are sent correctly by checking the routing table rebroadcasting is avoided.Then the data is transferred from the source to the destination.

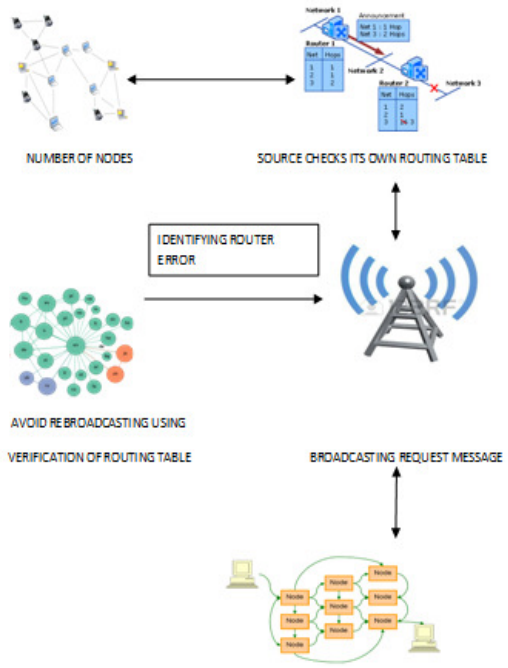

Fig.1 Architecture diagram of the Proposed system

V.ALGORITHM

This algorithm includes two forms in it.They are:

1.Request algorithm

2.Response algorithm

REQUEST ALGORITHM:

```
Class MeanQueryTime -superclass Simulator
MeanQueryTime instproc init {avgdelay_ mqgtime_} {
$self instvar avgdelay
$self instvar mqgtime
set avgdelay $avgdelay_
set mqgtime $mqgtime_
}
MeanQueryTime instproc MeanQGenTime {} {
$self instvar mqgtime
return $mqgtime
}
MeanQueryTime instproc Avg_Delay {} {
$self instvar avgdelay
return $avgdelay
}
## Getting send_Rxve_Pkts..
set mqgtime_ 10
```

```
set avgdelay_ [expr rand()*0.5]
set c [new MeanQueryTime $avgdelay_ $mqgtime_]
set averageDelay [$c Avg_Delay]
set mqgentime [$c MeanQGenTime]
```

RESPONSE ALGORITHM:

```
Class MeanQueryTime -superclass Simulator
MeanQueryTime instproc init {avgdelay_ mttltime_} {
$self instvar avgdelay
$self instvar mttltime
set avgdelay $avgdelay_
set mttltime $mttltime_
}
MeanQueryTime instproc MeanQGenTime {} {
$self instvar mttltime
return $mttltime
}
MeanQueryTime instproc Avg_Delay {} {
$self instvar avgdelay
return $avgdelay
}
## Getting send_Rxve_Pkts
set mttltime_ 10
set avgdelay_ [expr rand()*0.5]
set c [new MeanQueryTime $avgdelay_ $mttltime_]
set averageDelay [$c Avg_Delay]
set mttltime [$c MeanQGenTime]
```

VI.EFFECTS OF ATTACK MADE BY MALICIOUS NODES

The various types of attacks and the impact of these attacks are discussed in this section of the proposed work. In MANET a malign node can restrict the service of a perfect route between the source and the destination and hence the route becomes invalid and unnecessary traffic will be imposed in the network. The presence of such nodes make the other perfect nodes nullified [6].

Mobilising the packets among such network containing the malign nodes is a horrible task to maintain the proper functioning of the network without proper security systems. This can be done by isolating the nodes from the network after detecting and can be stopped from sending or receiving files through such nodes.

Deleting the malign node alone does not increase the performance of the network but the intermediate node should recognize and identify a trustworthy path between the source and the destination before the data transmission take place. The routing error can be done by the malign node by sending a fake route error message to its neighbouring nodes and thus misguiding them to choose a different path. Thus the network traffic is thus increased.

The nodes can also block the resources for them and causing the other nodes in the network starve for the resource. The table 1.1 shows the various activities performed by the malicious nodes.

TABLE.1.1 MALICIOUS ACTIVITIES PERFORMED BY INTERMEDIATE NODE

S.NO	ACTIVITY	FUNCTIONSDONE
1	Illegal Advertisement	Malign nodes can send fake message to its neighbours to misguide them
2	Source-Destination Delay	Intentionally drop packets during the transit between source and destination
3	Flooding	Send unnecessary queries in the network
4	Block Resources	Reserve resource for their own benefits.

The fig.2 shows the use case diagram of the malicious node.

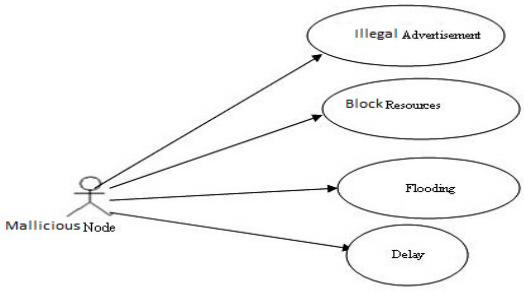

Fig.2 Use case of Malicious Node

For example let us consider a network as shown in the figure 3.

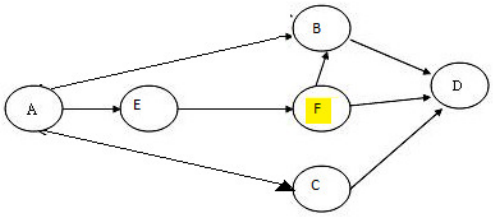

Fig. 3 Network with 6 Nodes with a Malicious Node F

The figure 3 shows the network with 6 nodes and a malicious node F. Now we need to analyse how the data is being transferred from the source A to the destination D through the various node and find the malicious node in the path from the source to destination.

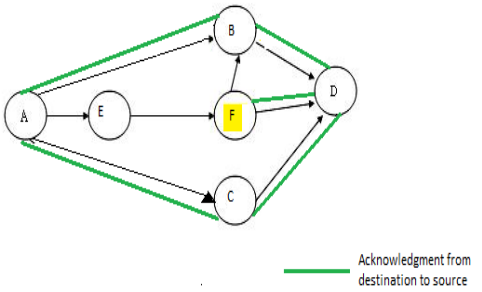

Fig.4 Acknowledgment from destination to source

Figure 4 shows the acknowledgment from the destination to the source through all the routes the data had reached the destination.

Case1: If A node is not receiving acknowledgement from particular route after sending number of packets to D.In Fig: 4, If A is not receiving ACK packets from path A->E->F->D, after sending number of packets in varying intervals of D. Whereas it is receiving acknowledgement from other paths like A->B->D and A->C->.D. In this case, there may be possibility of malicious node in path A->E->F->D.

Case 2: If malicious node F declares that it is having greatest destination sequence number than the destination node. Other nodes may assume that F is destination node and can easily divert the traffic towards F.

Case 3: If the node F is endlessly sending frequent and duplicated packets to other nodes then unnecessary traffic jam may occur.

Case 4: If confidence value of F, evaluated by its neighbours is less.

Case 5: If packet dropping ratio is high. Then malicious node may be present in this scenario

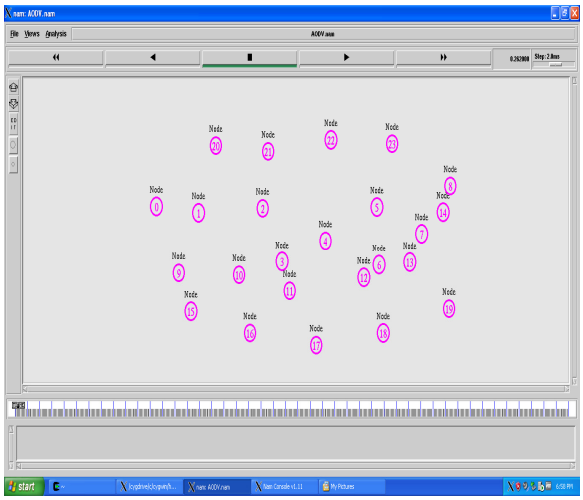

Fig. 5 shows how the nodes are constructed

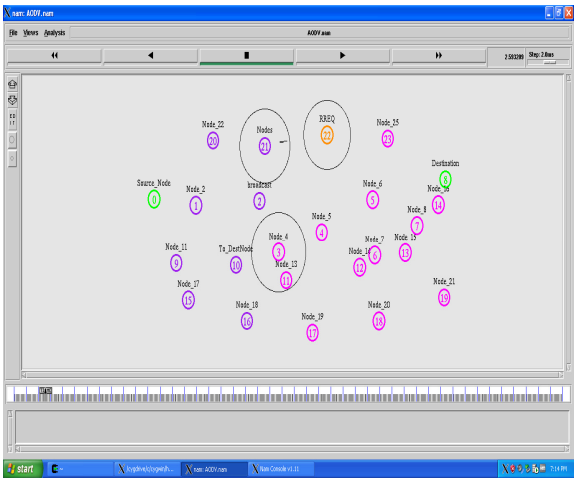

Fig.6 shows route selection based on RREQ

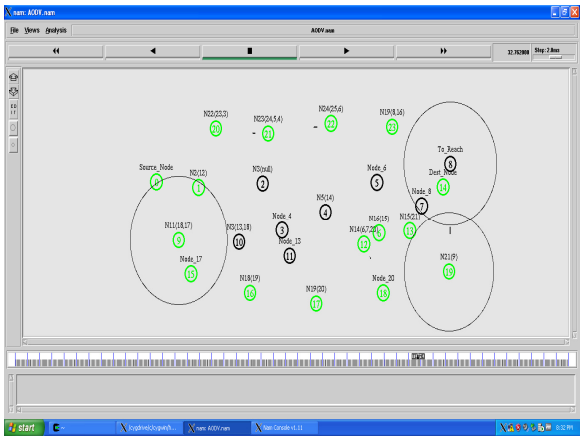

Fig.7 shows how the data is transmitted from source to destination

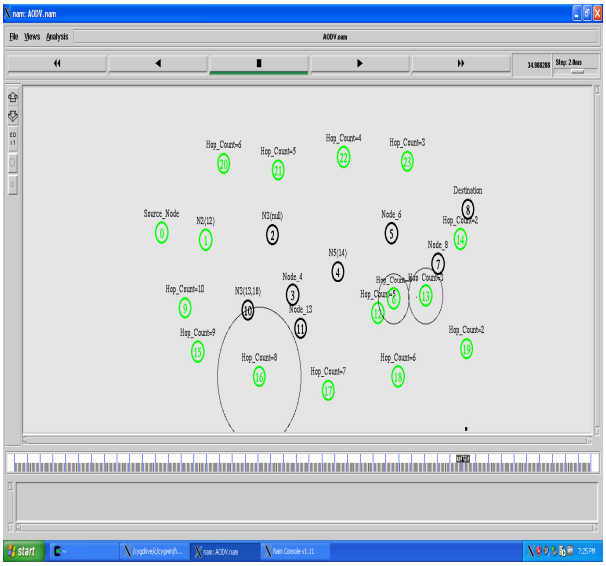

Fig.8 shows the route selection based on hop count

VII.MALICIOUS NODE ISOLATION

First the end nodes namely source and destination node finds malign nodes through EIDS-AODV technic as in [3]. The existence of malicious node is evaluated by these nodes using one hop and two hop distances.Each node that is in between the source and destination shall also follow the same process.Thus all links where malicious nodes are present is identified.The neighbours acknowledge the presence of malicious nodes.The neighbours broadcast this message to all neighbours immediately.Consequently all the nodes store the parameters of the malicious node in the parameter table.Then the path which is affected by the malicious node which is found is deleted, hence the route from source to destination containing the malicious node is deleted. Each intermediate node that want to remove a link, will broadcast this information to all its neighbors. The same is followed if other nodes also want to delete the node from the link.There by removal accuracy will be at its maximum. Otherwise, deleting the existing path or link is not possible without this.The existence of the link without removal decreases the performance of the network at any time t0 or t1 etc. Thus the path containing the malicious node is deleted from source routing table for improving the performance of the network.The isolated node is prohibited from participating in the network and transmitting the data from source to destination. After isolation the other nodes do not consider the malicious nodes as a intermediate node and it also does not accept the request received from these malicious nodes. Such malicious nodes are cutting them off from the entire network. After removal of the malign nodes the other part of the network remains intact and the network is re-tested.

VIII.RESULTS

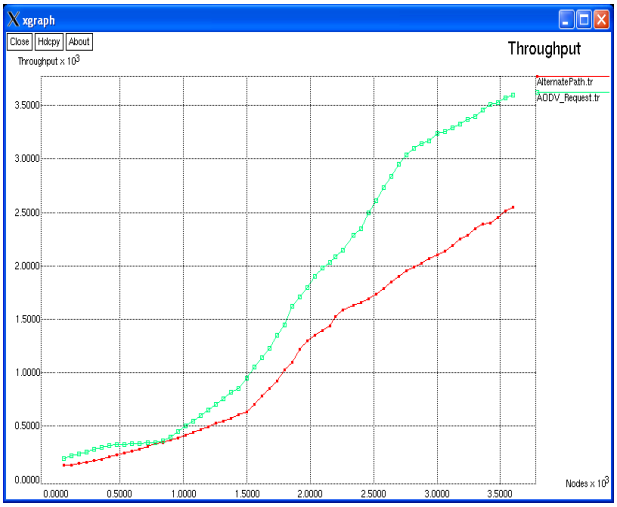

Fig.9 Graph showing the throughput

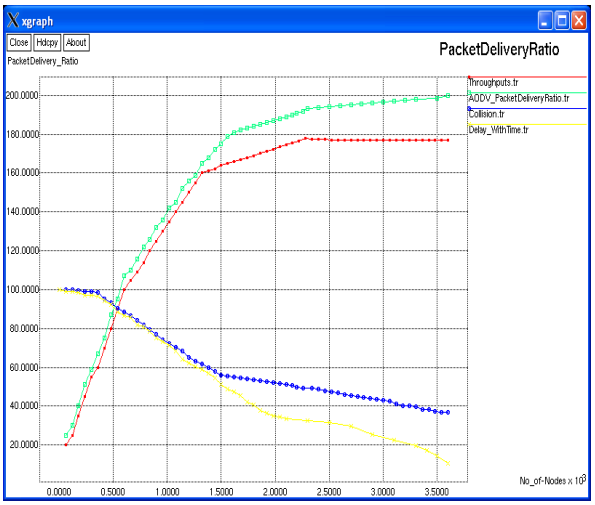

Fig.10 Graph showing the Packet delivery Ratio

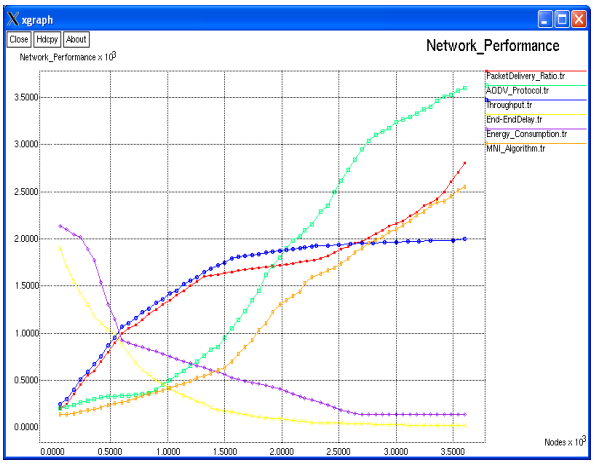

Fig.11 Graph showing the Network Performance

Fig.9 represents the throughput obtained from the processed data. Throughput is the one which determines the number of packets received successfully in a unit time and it is represented in bps.

Fig.10 represents the packet delivery ratio which is the ratio of the packets delivered successfully to the destination to the number of packets that have been sent by the sender.

Fig.11 represents the network performance which determines the efficiency of the network.

IX.DATAFLOW DIAGRAM

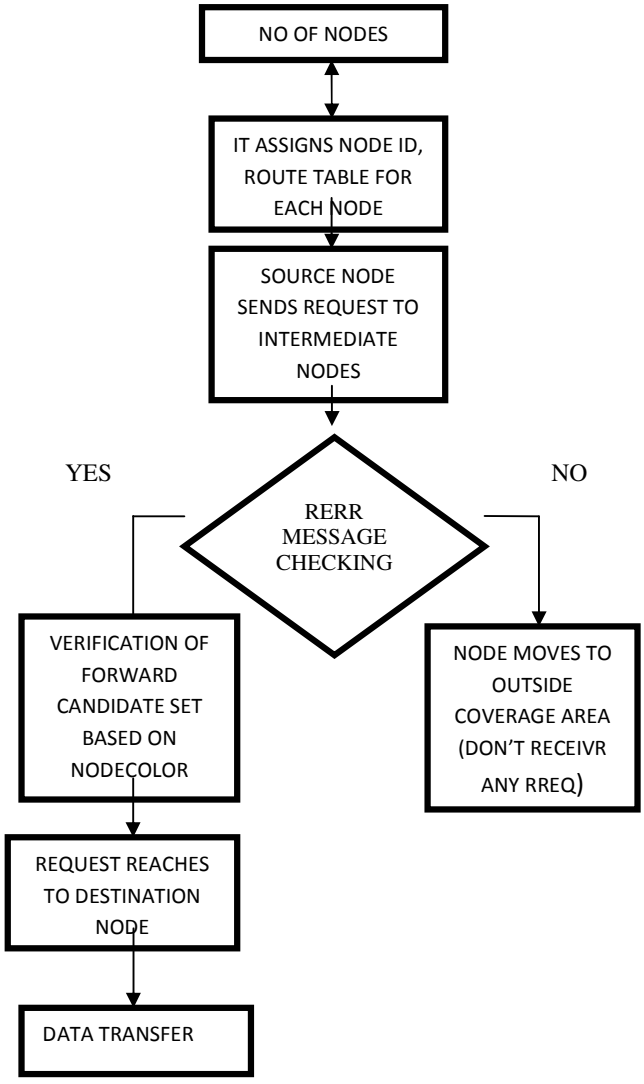

Fig.12 Dataflow diagram of proposed system

X. CONCLUSION

In conclusion, a malign node can misinterpret data anywhere in a network. In the process of discovering the route the malign node can add some fake data or drop some of the existing packets from the network. The malicious node identified should be isolated from the network without fail. Proposed approach EIDS-AODV and Enhanced AODV identifies malicious node where as MNI-AODV isolate malicious nodes. The isolation algorithm proposed here can be acted upon with other routing algorithms as well. In pace with the increased large mobility, ad hoc networks certainly have the potential to become very beneficial in coming future.

REFERENCES

[1] C.Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks", Pearson Publication ,2005.ISBN **81-297-0945-7**

[2] C.K.Toh, "Adhoc Mobile wireless networks: Protocols and Systems", Prentice Hall ,New Jersy,2002.

[3] Umang, Reddy B.V.R and Hoda M. N., "Enhanced IDS in Adhoc routing protocol using minimal energy Consumption", **ISSN-1751-8628**, DOI: 10.1049/iet-com.2009**.0616**, IEE Journal Communications IET, Volume 4, Issue 17, Nov, 2010 (Impact Factor- 0.963)

[4] Umang, Reddy B.V.R and Hoda M. N., "GNDA: Detecting Good Neighbor nodes in Adhoc Routing Protocol", **ISSN 978-0-7695-4329-1/11**/$26.00©IEEE, DOI: 10.1109/EAIT.2011.62, IEEE EAIT 2011, pp no 235-238.Feb 19-20, 2011

[5] Umang, Reddy B.V.R and Hoda M. N., "Vulnerability of Numerous Black Hole Nodes in Mobile Ad hoc Networks-Problem", IEEE International Advance Computing Conference", **ISBN: 978-981-08-2465-5**© IEEE , March, 2009.

[6] Umang, Reddy B. V. R and Hoda M. N; "Impact of malicious nodes in mobile adhoc networks using AODV routing, National Conference on "Advances in Wireless Cellular Telecommunications: Technologies and Services", organized by Institution of Communication Engineers and Information Technologists (ICEIT) Delhi, 14th -15th April, 2011.

[7] Umang,Dr. B V. R. Reddy and Dr. M .N. Hoda "MNI-AODV: Analytical Model for attack mitigation using AODV routing in ad hoc networks", 2014 International Conference on Computing for Sustainable Global Development (INDIACom)

[8] Muhammad Zeshan , Shoad A. khan'Adding Security Against packet dropping Attack in Mobile Ad hoc Networks', Proceedings of ACM International Seminar on Future Information Tech & Mgmt Engg (FITME 2008).

[9] Jaydip Sen , Girish Chandra. P 'A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks', Proceedings of IEEE International conference on Telecommunication(2007).

[10] Sirisha R. Medidi, Muralidhar Medidi & Sireesh Gavini'Detecting Packet-dropping Faults in Mobile Ad-hoc networks', **IEEE 2003**.

[11] S.Marti,T.Giuli,k.Lai,and M.baker,"Mitigating routing misbehaviour in mobile ad hoc networks",proceedings of international conference on mobile computing and networking,**AUG 2000.**

[12] Bhalaji .N & Dr. Shanmugam .A,'Reliable Routing Against Selective Packet Drop Attack in DSR Based MANET', **Journal of Software 2009.**

[13] K.liu.J.Deng, P.Varshney, K.balakrishnana, " An acknowledgment based approach for the detection of routing misbehaviour in MANETs", IEEE Transaction on mobile computing ,2007.