International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Performance of CBIDS on AODV Routing Protocol against Black hole attacks in MANET

R. Lakshmana Rao[1], Prof. B. Satyanarayana[2], B. Kondaiah[3]

[1]Research Scholar Department of Computer Science &Technology Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India

[2]Research Supervisor Department of Computer Science &Technology Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India

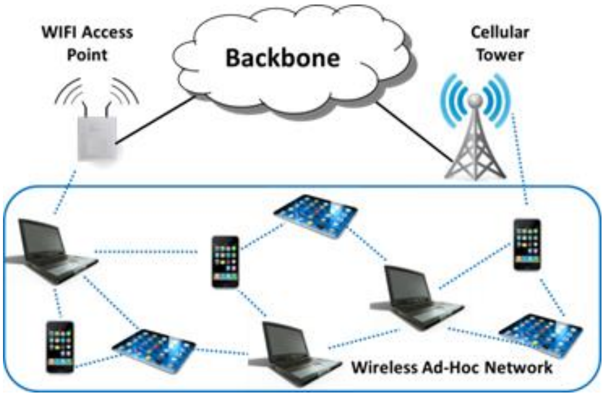
ABSTRACT

Mobile Ad hoc Networks (MANETs) are multi hop wireless adhoc networks, in which nodes are communicate with each other nodes without any centralized administration or base stations. Routing is defined as the process of finding path from a source to every destination in the network. There are three types of routing protocols in MANET such as reactive, proactive and hybrid routing protocol. Ad-hoc On-Demand Distance Vector (AODV) is a reactive routing protocol which is used for finding a efficient path to the destination in an ad-hoc network. MANETs faced different types of securities attacks that are carried out against them to interrupt and disturb the normal performance of the networks. The black hole attack is most dangerous active attack when occurs in network, it drops the data packets while transmission of data in MANET. In this paper we implemented Cache Based IDS on AODV Routing Protocol with black hole attack. The proposed routing protocol is designed using caching mechanism technique which prevents false replies from attacker nodes. The performance is tested for Pocket delivery ratio, pocket loss ratio and throughput for the proposed technique using ns2 simulation environment.

Keywords: MANET, AODV, CBIDS-AODV, Black hole Attack, NS2

I. INTRODUCTION

In a MANET, a collection of mobile nodes with wireless network interfaces form a temporary network without any fixed infrastructure or centralized. Due to lack of any kind fixed infrastructure and open wireless medium security implementation is difficult. In MANET each node functions as a host as well as router, forwarding packets for another node in the network. MANET is vulnerable to different kinds of attacks [6]. These include active route snooping, imprecation and denial of service. Black hole attack is one of the most dangerous attacks in MANET. In this attack, a malicious node sends a fake Route REPLY (RREP) packet to a source node which is not trustworthy that initiates the route discovery in order to imagine being a destination node [7]. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery process [1].



CSEIT1833629 | Received : 10 April 2018 | Accepted : 24 April 2018 | March-April-2018 [(3) 3 : 1637-1644]

Figure 1. Mobile Adhoc Network

Routing in Manet

Routing is defined as the process of finding path from a source to every destination in the network. There are three main requirements for designing ad hoc network routing protocols i.e. Low overhead, Adaptiveness and Resilience to loss. Manet routing protocols are classified into various types based on different criteria.

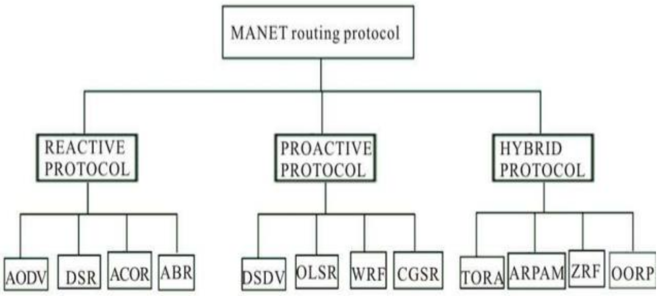


Figure 2. Classification of Routing Protocols

II. ADHOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV is an on demand distance vector routing protocol. In on demand routing a route is established between communicating nodes only. There is no fixed existing route as in table driven systems. Whenever a node needs to send data packets it has to initiate route discovery process. Route discovery consists of two messages: Route Request (RREQ) and Route Reply (RREP).

The source node broadcasts the RREQ messages to its neighbors which further broadcasts them to their neighbors and so on [2]. In response to RREQ, either the destination node replies with RREP or intermediate node having route to destination replies with RREP [8]. When intermediate node replies it is called unwarranted Route Reply. Validity and freshness of route is decided by destination sequence number. If destination sequence number is higher than before than route is considered valid. Source selects the path for data packets transmission from which it received RREP first. Further received RREPs are discarded.

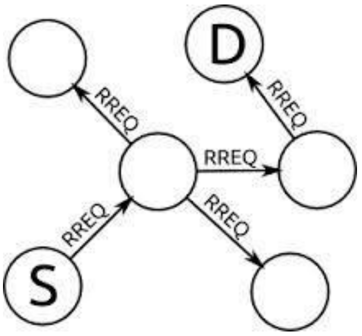


Figure 3. Aodv routing protocol with RREQ

With RREQ and RREP message. For route maintenance nodes sporadically send HELLO messages to neighbor nodes [12]. If a node fails to receive three successive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node.

Security Issues in Manet

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met [9]. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats [3]. There are several types of attacks such as black hole and wormhole.

Black hole Attack

A Black hole attack is a kind of denial of service where a malicious node can attract all packets by fallaciously claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Cooperative Black hole means the malicious nodes act in a group [5]. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the adjacent nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP [10]. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets [11]. On the receiving of data packets, the Black hole node simply drops them, instead of forwarding to the destination.

In black hole attack a malicious node can be detects the active route and notes the destination address or can be sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node [4]. The new information received in the route reply will allow the source node to update its routing table. New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route.

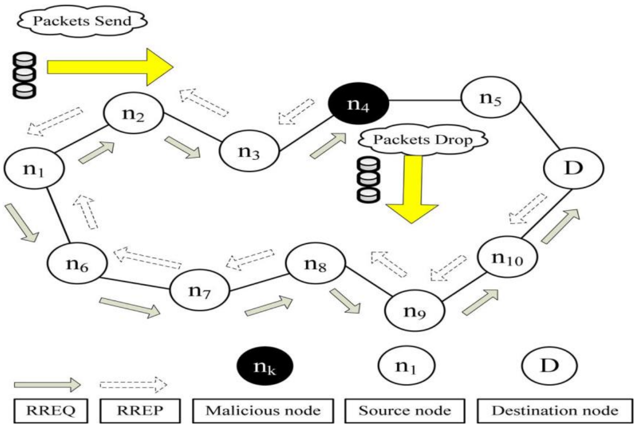


Figure 4. Dropping the packets by Black hole attack

Implementation of AODV Algorithm with Black hole attack

Step 1: Suppose S is a source and D is destination and S wants to send data to D.

Step 2:When S wants to send data to destination then it will send request to destination. If that node is a valid destination then it will send reply to the source.

Step 3: RTRPLYN (Route Reply Node) is the intermediate node between source and destination. Then it will send verify packet to destination node.

Step 4: When S receives RTRPLY (Route Reply), then it will send a CHECKVRF (Check Verification) packet to D via a path suggested by RTRPLYN.

Step 6: When D gets VERIFY packet from intermediate node, it stores its contents in a table to Prepare Final reply.

Step 7: When D receives CHECKVRF packet from S, it checks in table if it got any VERIFY packet with matching source ID.

Step 8: If it matches, it sends a FINALREPLY packet.

Step 9: In case of black hole, FINALREPLY packet will not reached the source because VERIFY and CHECKVRF packets are not forwarded to the destination node.

III. SOLUTION FOR BLACK HOLE ATTACK AND ITS EFFECTS

In the two previous chapters, we explain how Black Hole Attack is implemented in NS2 and which the results are obtained from the simulations. When we examine the trace file of the simulations that include one black hole node, followed by RREP messages received by source node from the active nodes (destination/intermediate node) we saw that after a while second RREP message came to source node from the real destination node. The Table.1 shows the route reply message represents of in presence of black hole attack.

Table 1. Receiving two RREP messages

			MAC Header		IP Header		AOVD Packet			
Event	Time (-t)	Node ID (-Ni)	Destination Address	Souce Address (-Ms)	Destination IP.Port	Source IP.Port Address	Packet Type (-Pc)	Destination Node	Destination Seq No	Hop Count (-Ph)
R	0.205976 533	0	0	1	0.255	1.255	REPLY	5	-1	1
R	1.276544 080	0	0	2	0.255	5.255	REPLY	5	4	4

Description of functions

recv:- It is a function that processes the packets based on its type. If packet type is any of the many AODV route management packets, it sends the packet to the "recvAODV" function.

RecvblackholeAODV:- It is a function and it checks the type of the AODV management packet and based on the packet type it sends them to appropriate function with a "case" statement.

recvRequest:- This function is used for receiving RREQ message from source node

recvReply:- This function received RREP message from destination node.

rrep_insert:- This function is used for adding RREP messages.

rrep_lookup:- This function is used for for looking any RREP message up if it is existed or not.

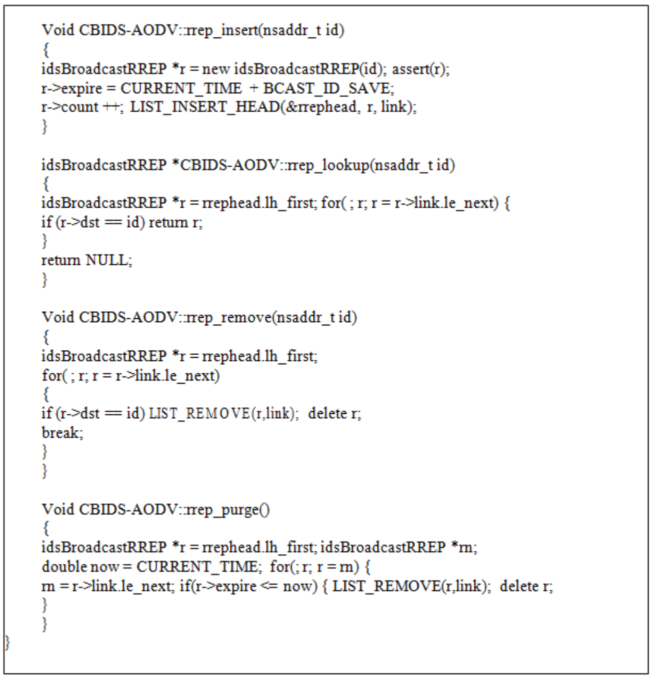
rrep_remove:- This function is used for removing any record for RREP message that arrived from defined node.

rrep_purge():- This function is to delete periodically from the list if it has expired

Introduction to CBIDS-AODV

In this proposed method we have implementing CBIDS-AODV protocol against black hole attack in manet. In AODV with black hole attack, it explained how black hole attack is implemented in NS2 and the results are obtained from the simulations. When we examine the trace file of the simulations that include one black hole node, we observe that after a while second RREP message comes to source node from the real intermediate node. To figure out how the second packet came to source node, it has been created a simulation scenario with node positions. In the scenario, Node 0 is the sending node, Node 1 is black hole node and node 4 is the receiving node. As the black hole send an RREP message without checking the tables, we assume that it is more likely for the first RREP to arrive from the black hole. In some cases, this idea may not work. For instance; the second RREP can be received at source node from an intermediate node which has fresh enough information about the destination node or the second RREP message may also come from the black hole node if the real destination node is nearer than the black hole node or in networks with multiple black hole nodes, second RREP can receive from other black hole nodes. Implementation of CBIDS-AODV to evaluate effects of the proposed solution, first it needs to implement in NS-2. Therefore, should simulate the "aodv" protocol, changing it to "CBIDS-AODV" as it did "blackholeaodv" before.

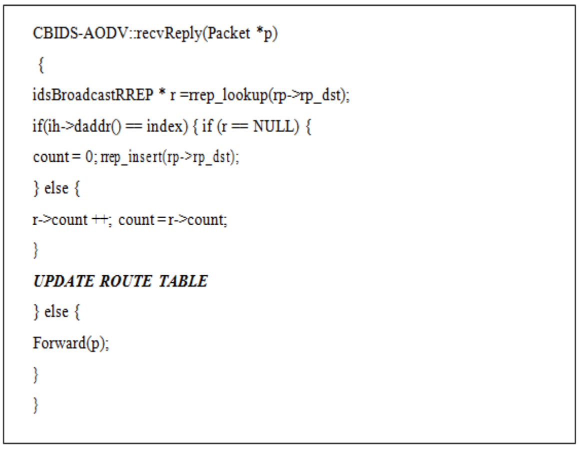
To implement this black hole attack has been changed the receive RREQ function (recvRequest) of the blackholeaodv.cc file but to implement the solution had to change the receive RREP function (recvReply) and create RREP caching mechanism to count the second RREP message. The RREP caching mechanism "rrep_insert" function is for adding RREP messages, "rrep_lookup" function is for looking any RREP message up if it is exist, "rrep_remove" function is for removing any record for RREP message that arrived from defined node and "rrep_purge" function is to delete periodically from the list if it has expired. It's chosen that this expiry time "BCAST_ID_SAVE" as 6 (takes seconds).



```
Void CBIDS-AODV::rrep_insert(nsaddr_t id)
{
idsBroadcastRREP *r = new idsBroadcastRREP(id); assert(r);
r->expire = CURRENT_TIME + BCAST_ID_SAVE;
r->count ++; LIST_INSERT_HEAD(&rrephead, r, link);
}

idsBroadcastRREP *CBIDS-AODV::rrep_lookup(nsaddr_t id)
{
idsBroadcastRREP *r = rrephead.lh_first; for( ; r; r = r->link.le_next) {
if (r->dst == id) return r;
}
return NULL;
}

Void CBIDS-AODV::rrep_remove(nsaddr_t id)
{
idsBroadcastRREP *r = rrephead.lh_first;
for( ; r; r = r->link.le_next)
{
if (r->dst == id) LIST_REMOVE(r,link);  delete r;
break;
}
}

Void CBIDS-AODV::rrep_purge()
{
idsBroadcastRREP *r = rrephead.lh_first; idsBroadcastRREP *rn;
double now = CURRENT_TIME;  for(; r; r = rn) {
rn = r->link.le_next; if(r->expire <= now) { LIST_REMOVE(r,link);  delete r;
}
}
}
```

Figure 5. RREP Caching Mechanism

In the "recvReply" function, we first control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived. If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is cached before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbor. Figure. 5 shows how the receive RREP message function of the CBIDS-AODV is carried out.



```
CBIDS-AODV::recvReply(Packet *p)
 {
idsBroadcastRREP * r =rrep_lookup(rp->rp_dst);
if(ih->daddr() == index) { if (r == NULL) {
count = 0; rrep_insert(rp->rp_dst);
} else {
r->count ++; count=r->count;
}
UPDATE ROUTE TABLE
} else {
Forward(p);
}
}
```

Figure 6. Receive RREP function of the CBIDS-AODV

3.3. Testing the CBIDS-AODV

Having implemented the CBIDS-AODV protocol in NS-2, we tried it in a tcl simulation. In the scenario of the simulation there are seven motionless nodes and node positions are the same as in the test simulation of the two RREP messages, shown in Figure 5. In this simulation CBIDS-AODV protocol is used instead of AODV for all nodes except the black hole node (Node 1). To change the AODV protocol to CBIDS-AODV we only change "$ns node-config -adhocRouting CBIDS-AODV". When the simulation is compiled, we saw that sending node is sending the messages to receiving node properly.

Network Simulator (NS2)

The proposed protocol evaluations are based on Network Simulator (NS2). NS2 can be used to simulate a wide variety of network protocols, traffic sources. It also supports a wide variety of static and dynamic routing protocols. NS2 can also be used to implement multicast on demand routing protocols and it also supports the multipath routing protocols. Network Simulator is an Object Oriented Tool command language (OTcl). It is a script interpreter which contains a simulation event scheduler and network component object libraries in addition to network setup (plumbing) module libraries.

Table 2. Simulation parameters

Parameter	Value
NS2 version	2.35
Topography	800m * 800m
Number of Nodes	20
Routing Protocol	AODV
Simulation Time	500s
Packet size	512 bytes
Application traffic	CBR
Mobility	Random way point

Performance metrics

AODV routing Protocol is used for simulation in various network densities and node distribution. It is assumed that link between nodes is bidirectional and circular. The performance can be measured by variety of metrics like packet delivery ratio, packet loss ratio and throughput on AODV and CBIDS-AODV with black hole attack.

Packet Delivery Ratio:-

The ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDF shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

$$\text{packetdelivery ratio} = \frac{\sum \text{No. of packets received}}{\sum \text{No. of packets sent}} * 100$$

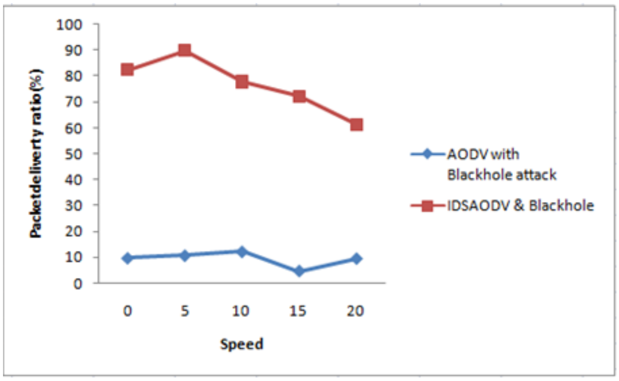


Figure 7. Packet delivery ratio of AODV and CBIDS-AODV

The Figure 7 shows that the result of Packet Delivery Ratio on performance of AODV and CBIDS-AODV routing protocols with black hole attack. In this graph the X value represents speed (0, 5, 10, 15 and 20) milliseconds and Y represents ratio of packets delivered. In the above result the CBIDS-AODV packet delivery ratio is very high because of implementing intrusion detection scheme using AODV routing protocol in the network.

Packet Loss Ratio

Packet loss is the number of packets dropped or lost per unit time during simulation. Low value of packet loss corresponds to the better performance of the protocol.

$$\frac{(\sum \text{No. of Packets sent} - \sum \text{No. of packets received})}{(\text{stop time} - \text{start time})}$$

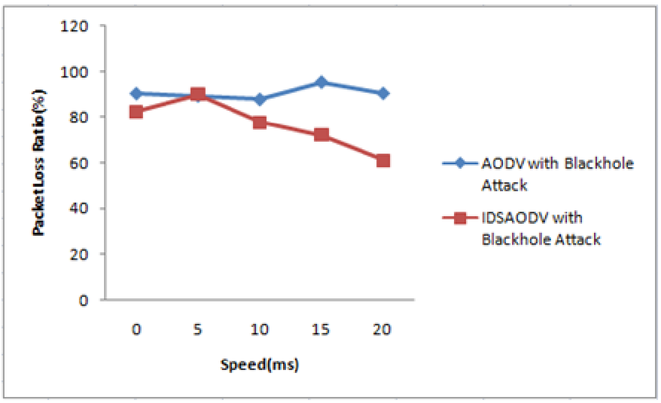


Figure 8. Packet Loss Ratio on AODV & AODV with Black hole Attack

The Figure 8 shows that the result of Packet Loss Ration on performance of AODV and CBIDS-AODV routing protocols with black hole attack. In this graph the X value represents speed (0, 5, 10, 15 and 20) milliseconds and Y represents ratio of packets dropped. In the above result the CBIDS-AODV packet loss ratio is very low because of implementing intrusion detection scheme using AODV routing protocol in the network.

Throughput

Throughput is the number of packet that is passing through the channel in a particular unit of time. This performance metric show the total number of packets that have been successfully delivered from source node to destination node and it can be improved with increasing speed.

$$\text{Throughput} = \frac{(\text{No. of data packets received} * \text{packet size} * 8)}{\text{Simulation time}}$$

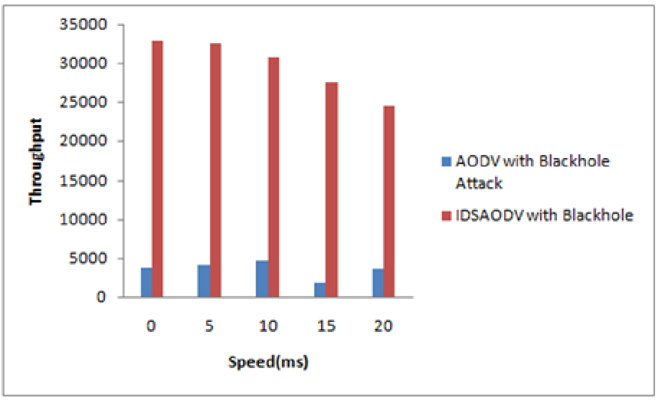


Figure 9. Throughput of AODV and CBIDS-AODV

The Figure 9 shows that the result of Throughput on performance of AODV and CBIDS-AODV routing protocols with black hole attack. In this graph the X value represents speed (0, 5, 10, 15 and 20) milliseconds and Y represents No. of bits transmitted in simulation time. In the above result the CBIDS-AODV throughput is very high because of implementing intrusion detection scheme using AODV routing protocol in the network.

IV. CONCLUSION AND FEATURE SCOPE

This paper presents the analysis and effect of blackhole attack on the performance of AODV and CBIDS -AODV routing protocols in MANET. It can be inferred that the Black Hole attack affect both the routing protocols. However it is concluded the proposed method as shown better performance against the AODV in terms of packet delivery ratio, packet loss ratio and throughput. Its detection is the main issue of concern. Therefore the work can be extended by implementing fuzzy logic or neural network mechanisms for more efficient to detect the Black Hole attack. Improvement for overcoming the affect of Black Hole should orient towards controlling the delay. In future the performance of the proposed routing protocol can be extended for better scalability using fuzzy logic and neural networks.

V. REFERENCES

[1]. Dharman,V G. Venkatachalam "Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest"South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 321-329, ISSN No:

[2]. Gourav Ahuja, Mrs. Sugandha "A Review on Black Hole Attack in MANET" International Journal of Advance Research in Science and Engineering, Vol.No.6,Issue No.07,July 2017,www.ijarse.com,ISSN(0)2319-8354, ISSN(P)2319-8346.

[3]. Gurbir Singh, Nitin Bhagat "Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-6, June 2015..

[4]. Dr. Gurjar, A. A. Dande, "BlackHole Attack in Manet's: A Review Study" International Journal of IT,Engineeriing and Applied Science Research(IJIEASR) ISSN: 2319-4413 Volume 2, No.3, March 2013i-Xplore International Research Journal Consortium www.irjcjournals.org.

[5]. Mrs.Jhansi,M Ms. K.RoopaDevi, Mr.B.Mukesh Chandra, "Effective Measure to Prevent Cooperative Black Hole Attack in Mobile Ad-hoc Wireless Networks" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 4, July-August 2012, pp.204-209.

[6]. Monika , Swati Gupta "Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 7 July 2015, Page No. 13268-13272.

[7]. Ms. Naveena, A Dr. K. Ramalinga Reddy "Dynamic Training Intrusion Detection Scheme for Black hole Attack in MANETs"International Journal of Engineering

Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012, pp.622-627

[8]. Ravindra Saini, P. Sunitha Devi" Malicious Node Detection in MANETs using Cooperative Bait Detection Approach and Trust Model" International Journal of Research and Scientific Innovation (IJRSI) |Volume III, Issue VIII, August 2016|ISSN 2321-2705.

[9]. Sapna Choudhary,Alka Agrawal "Threshold Based Intrusion Detection System for MANET using Machine Learning Approach" International Journal of Advance Electrical and Electronics Engineering (IJAEEE),ISSN (Print): 2278-8948, Volume-3 Issue-1, 2014.

[10]. SUSHIL KUMAR CHAMOLI, SANTOSH KUMAR, DEEPAK SINGH RANA, "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" Int.J.Computer Technology & Applications,Vol 3 (4), 1395-1399, ISSN:2229-6093.

[11]. Sushil Kumar,Deepak Singh Rana, Sushil Chandra Dimri, "Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET" International Journal of Computer Applications (0975 - 8887) Volume 124 - No.1, August 2015.

[12]. Dr.Tamilarasan S "Securing AODV Routing Protocol from Black Hole Attack" International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012