Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

Prevention and Detection of Blackhole Attack in MANET using Modified AODV Protocol

Prof.M.B.Lonare[1], Anil Choudhary[2], Chehel Sharma[3], Ershad Mulani[4], Harish Yadav[5]

[1,2,3,4, 5]*Department of Computer Engineering, Army Institute of Technology, Pune, India*

Abstract *—This report gives information about the detection and prevention technique of black hole in the MANET using AODV protocol. An ad-hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates without the central administration. Hence it becomes more susceptible to the attacker. Ad-Hoc On demand Distance Vector (AODV) protocol is frequently used on- demand routing protocol used in Ad-Hoc networks. The security of the Ad-Hoc On demand Distance Vector protocol is breached by a type of attack known as "Black Hole" attack. In this kind of attack, a malicious node expresses itself as owning the shortest path to the node whose packets it wants to collect and intercept. To find a safe route and to drastically reduce the intercepting probability, it is proposed to wait and check for all the replies from the neighbouring nodes. There are many mechanisms of detection to eliminate the intruder (attacker) that perpetrate blackhole attack present in network. In this thesis, we have emulated the blackhole attack in various Mobile Ad-hoc network scenarios, have the detected malicious node present in the network using modified AODV protocol and shown the Performance Evaluation.*

Keywords--*Mobile ad-hoc routing, BlackHole, Detection methods, Emulation, AODV protocol, Performance Evaluation*

I. INTRODUCTION

A mobile ad-hoc network is a self-organizing network that consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. On the contrary to traditional wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals. Ad hoc Networks are the networks formed for a particular purpose. These networks assume that an end to end path between the nodes exists. They are often created on-the-fly and for one-time or temporary use. They find their use in special applications like military, disaster relief and are in a need of forming a new infrastructure less network with all pre-existing infrastructure being destroyed.

Wireless ad-hoc networks are composed of autonomous nodes that are self-managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbour nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. The attack that we implement is the well known attack called BlackHole attack. We have simulated packet loss problem by Node Failure, Distance Range and Network Congestion and determines how many packets are losses in the network. AODV uses two type's parameters i.e. sequence number and hop count for forwarding routing control packets. Sequence number describes the fresh information of the network and hop count shows shortest routes. AODV routing protocol prefers freshers routes comparison shorter routes so malicious node takes the advantage assigning big sequence number in a route reply message and able to redirect the route.

In addition to this, we have simulated Black Hole Attack on AODV routing and also proposed its detection method and determined network performance under different network scenario. In our study, we simulated the Black Hole attack in wireless ad-hoc net-works and evaluated its damage in the network. We made our simulations using NS-2.34 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the

existing network topologies. Even though NS-2.34 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first modified AODV routing protocol to simulate Black Hole attack in NS-2. We started our study by modifying AODV protocol using C++, to simulate the Black Hole attack.
Having implemented malicious node in AODV routing protocol which simulates the black hole attack we performed tests on different topologies to compare the network performance with and without black holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a malicious node. Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2. and evaluated the results as we did in Black Hole implementation. As a result, our solution is eliminated the Black Hole effect with 24.38 percentage success.

II. PROBLEM DESCRIPTION

Ad-hoc network is a collection of dynamic nodes it means any node can join the network and leave the network any time. Wireless communication is less secure than wired communication and that's why it is the vulnerability of mobile ad-hoc network and any threat can easily affect the communication. Many types of attacks are developed today which badly crash the network and make the communication performance degrade. So for avoid these vulnerabilities and make network secure we propose the technique on the security of mobile ad-hoc network by modifying the current protocols for blackhole detection in MANET. To provide the security of mobile ad-hoc network we generate new techniques for detection and prevention of black hole attack. Black hole attack is type of malicious node who drops the packet instead to send that packet to their destination. In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. We provide a detailed description herein.

III. LITERATURE SURVEY

1. Black Hole Attack in AODV:

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours. Imagine a malicious node „M". When node "A" broadcasts a RREQ packet, nodes "B" "D" and "M" receive it. Node "M", being a malicious node, does not check up with its routing table for the requested route to node "E". Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node "A" receives the RREP from "M" ahead of the RREP from "B" and "D". Node "A" assumes that the route through "M" is the shortest route and sends any packet to the destination through it. When the node "A" sends data to "A", it absorbs all the data and thus behaves like a "Black hole".

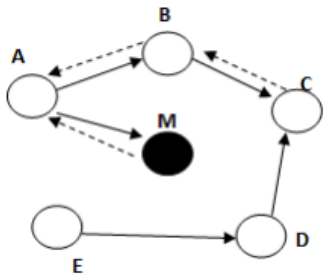

Figure 1. Black Hole Attack

2. Black Hole Attack in MANET:

Black Hole Attack in MANET:
Black hole attack is a type of MANET attack which present in a network and act as a true node but the true definition of black hole attack is a malicious node. Malicious node act as false node in the network and show that node has the best path for send the packet or says that it having fresh route to the destination. Source node broadcasts RREQ packet and further forwarded to intermediate nodes to search the best and short path. If the malicious is present in the network and if that node receive RREQ packet, it immediately sends false RREP packet with high sequence number. In this the false node claims that node has the best path for send the packet Thus the false node drops instead send the packet to its destination. In this Figure 2 the Black hole attack explains, the source node is node 1 and destination node is 4 and 3 is a

malicious node who act as an honest node. When source node send the request packets to all nodes than malicious node first of all give the reply and take the packet from source and drop the packet instead send that packet to destination node.

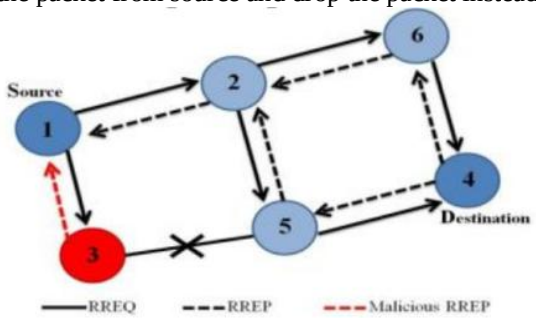

Figure 2. Black Hole Attack

The black hole attack is very serious type of attack that direct effect on the communication and packet delivery ratio and delay with throughput. Their different types of black hole attacks like as the cooperative black hole attack and single black hole attack.

IV. SOFTWARE REQUIREMENTS

Ubuntu
Ubuntu is different from the commercial Linux offerings that preceded it because it doesn't divide its efforts between a high-quality commercial version and a free 'community' version. The commercial and community teams collaborate to produce a single, high-quality release, which receives ongoing maintenance for a defined period. Both the release and ongoing updates are freely available to all users.We are using 14.04.1 version of ubuntu.
Network simulator
NS2 Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless net-work functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. We are using NS2.35.
TRGraph
Tracegraph is a third party software helps in plotting the graphs for NS2 and other networking simulation softwares. But the sad point is the software is not maintained by anyone and the happiest point is the software works fine still and it is free.

V. IMPLEMENTATION

To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit black hole behaviour in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Black Hole they have to use a new routing protocol that can participate in the AODV messaging.

Implementation of this new routing protocol is explained below in detail:
All routing protocols in NS are installed in the directory of "ns-2.29". We start the work by duplicating AODV protocol in this directory and change the name of directory as "blackholeaodv". Names of all files that are labeled as "aodv" in the directory are changed to "blackholeaodv" such as blackholeaodv.cc, blackholeaodv.h, blackholeaodv.tc l , blackholeaodv_rqueue.cc, blackholeaodv_rqueue.h etc. in this new directory except for "aodv_packet.h". The key point in our work is that AODV and Black Hole AODV protocol will send each other the same AODV packets. Therefore, we did not copy "aodv_packet.h" file into the blackholeaodv directory. We have changed all classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code. We have designed aodv and blackhole aodv protocols to send each other aodv packets. These two protocols are actually the same. After the above changes, we have changed two common files that are used in NS-2 globally to integrate new blackholeaodv protocol to the simulator. More files are changed to add new routing protocol and this new protocol uses its own packets. But in our implementation we do not need to add a new packet. Therefore we have changed only two files. The changes are explained below.


```
BlackholeAODV {
set ragent [$self create-blackholeaodv-agent $node]
}
Simulator instproc create-blackholeaodv-agent { node } { set
ragent [new Agent/blackholeAODV [$node node-addr]]
$self at 0.0 "$ragent start" # start BEACON/HELLO Messages
$node set ragent_ $ragent
return $ragent
}
```

Figure 3. "blackholeaodv" protocol agent is added in "\tcl\lib\ ns-lib.tcl"

```
blackholeaodv/blackholeaodv_logs.o
blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o
blackholeaodv/blackholeaodv_rqueue.o \
```

Figure 4. Addition to the "\makefile"

The First file modified is "\tcl\lib\ ns-lib.tcl" where protocol agents are coded as a procedure. When the nodes use blackholeaodv protocol, this agent is scheduled at the beginning of the simulation and it is assigned to the nodes that will use black hole aodv protocol. The agent procedure for blackholeaodv is shown in Figure 3. Second file which is adapted is "\makefile" in the root directory of the "ns-2.29".After all implementations are ready, we have to compile NS-2 again to create object files. We have added the above lines in Figure 4 to the "\makefile".

So far, we have implemented a new routing protocol which is labelled as blackholeaodv. But Black Hole behaviours have not yet been implemented in this new routing protocol. To add Black Hole behaviour into the new AODV protocol we made same changes in blackholeaodv/blackholeaodv.cc C++ file. We will describe these changes we made in blackholeaodv/blackholeaodv.cc file explaining working mechanism of the AODV and Black Hole AODV protocols below. When a packet is received by the "recv" function of the "aodv/aodv.cc", it 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 that we will explain below. If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a Black Hole it drops all data packets as long as the packet does not come to itself. In the code below, the first "if" condition provides the node to receive data packets if it is the destination. The "else" condition drops all remaining packets. If statement is shown in Figure 5.

```
if ( (u_int32_t)ih->saddr() == index)
forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY); else


drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 5. "If" statement for dropping or accepting the packets

If the packet is an AODV management packet, "recv" function sends it to "recvblackholeAODV" function. "recvblackholeAODV" function checks the type of the AODV management packet and based on the packet type it sends them to appropriate function with a "case" statement. For instance; RREQ packets are sent to the "recvRequest" function, RREP packets to "recvReply" function etc. case statements of "recvblackholeAODV" function is shown in Figure 6.


```
case AODVTYPE_RREQ:
recvRequest(p);
break;
case AODVTYPE_RREP:
recvReply(p);
break;
case AODVTYPE_RERR:
recvError(p);
break;
case AODVTYPE_HELLO:
 recvHello(p);
break;
default:
fprintf(stderr, "Invalid blackholeAODV type (%x)\n",
ah>ah_type);
exit(1);
```

Figure 6. Case statement for choosing the AODV control message types

```
sendReply(rq->rq_src,        // IP Destination
1,                           // Hop Count
index,                       // Dest IP Address
4294967295,                  // Highest Dest Sequence Num
MY_ROUTE_TIMEOUT,            // Lifetime
rq->rq_timestamp);           // timestamp
```

Figure 7. False RREP message of Black Hole Attack

In our case we will consider the RREQ function because Black Hole behaviour is carried out as the malicious node receives an RREQ packet. When malicious node receives an RREQ packet it immediately sends RREP packet as if it has fresh enough path to the destination. Malicious node tries to deceive nodes sending such an RREP packet. Highest sequence number of AODV protocol is 4294967295, 32 bit unsigned integer value. Values of RREP packet that malicious node will send are described below. The sequence number is set to 4294967295 and hop count is set to 1. The false RREP message of the Black Hole Attack is shown in Figure 7.

After all changes are finished we have re-compiled all NS-2 files to create object files. Having finished compilation, we have a new test bed to simulate Black Hole Attack in AODV protocol. In the next chapter we will describe the simulations and simulation results.

VI. SIMULATION

Simulation using the us command we compile the tcl file and generate two separate files ie i.e. trace file with tr extension and nam file with nam extension. We can visually simulate the network by opening the nam file by following command

```
ns aodv18.tcl          //for compiling the tcl file
nam aodv.nam           //for visually simulate the network
```

Figure 8. Attack Screenshot

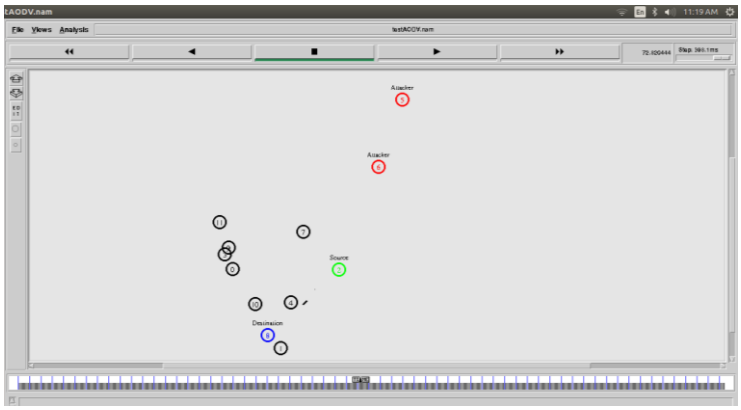

Figure 9. Prevent Screenshot

VII. RESULTS

★ **Network Details Comparison**

★

Network with Blackhole node

Node details:

Options Network information

Simulation information:

Simulation length in seconds:	93.03522921
Number of nodes:	12
Number of sending nodes:	12
Number of receiving nodes:	2
Number of generated packets:	53
Number of sent packets:	52
Number of forwarded packets:	6
Number of dropped packets:	7
Number of lost packets:	8
Minimal packet size:	40
Maximal packet size:	48
Average packet size:	47.082
Number of sent bytes:	2400
Number of forwarded bytes:	264
Number of dropped bytes:	288
Packets dropping nodes:	0 5 6

Current node information:

Number of generated packets:	4
Number of sent packets:	4
Number of forwarded packets:	0
Number of received packets:	29
Number of dropped packets:	5
Number of lost packets:	0
Number of sent bytes:	176
Number of forwarded bytes:	0
Number of received bytes:	1352
Number of dropped bytes:	200
Minimal packet size:	40
Maximal packet size:	48
Average packet size:	46.303

Figure 10. Attacker Node Details

Network without BlackHole node

Node details:

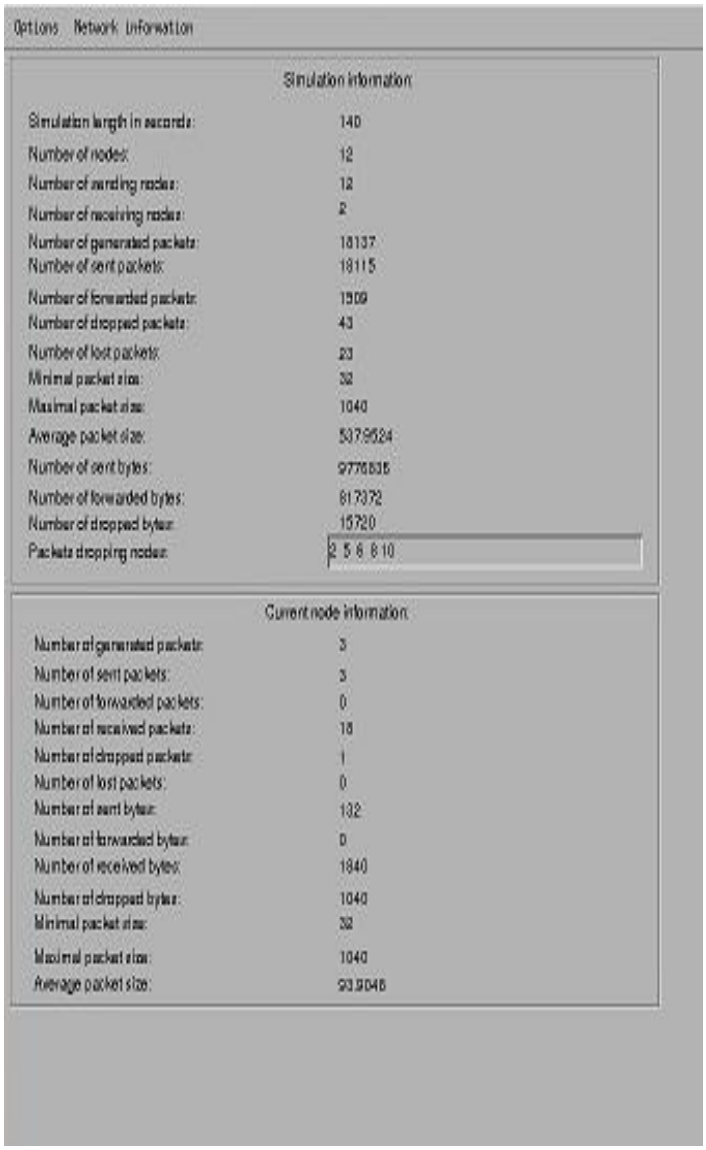

Figure 11. Node details after removal of Blackhole

Dropping Packet:

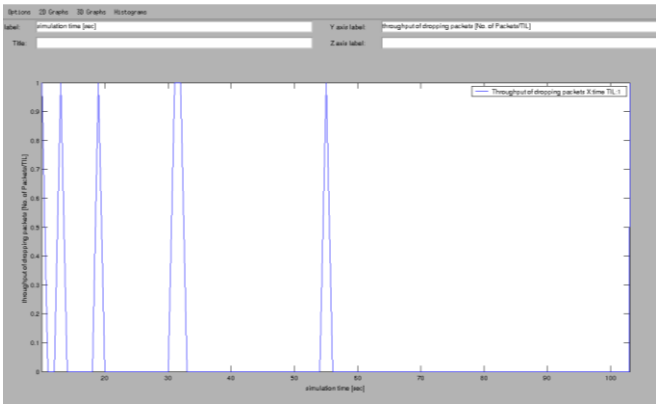

Figure 12. Packet drop graph while Black Hole

Dropping Packet:

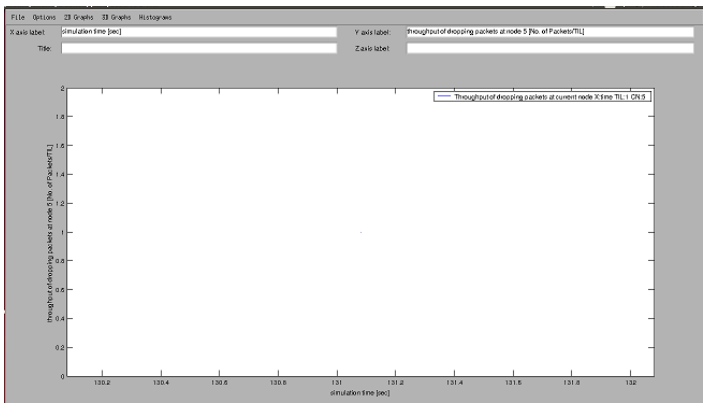

Figure 13. Packet drop graph after was present removal of Black Hole node

Throughput Details:

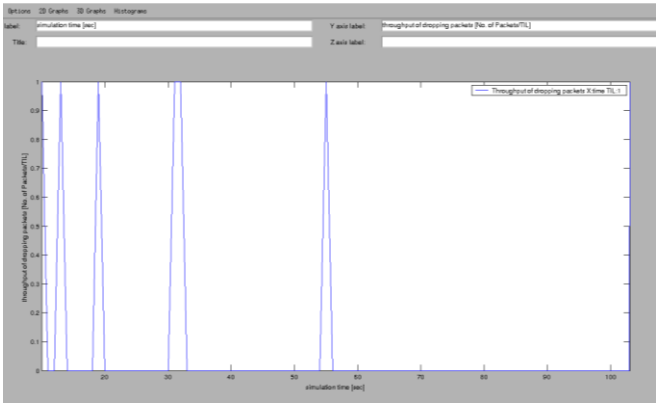

Figure 14. Throughput Details while Black Hole removal of Black Hole node

Throughput Details:

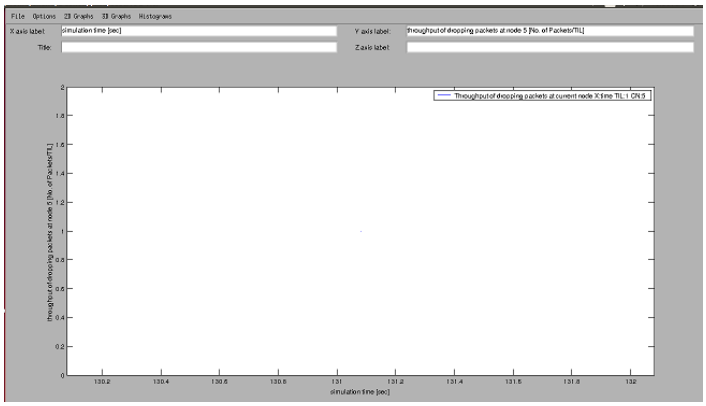

Figure 15. Throughput Details after was present

VIII. CONCLUSION AND FUTURE WORK

In this study, we analyzed effect of the Black Hole in an AODV Network. For this, we implemented an AODV protocol that acts as Black Hole in NS-2. We emulated a few scenarios where each one has 12 nodes that use AODV protocol and also emulated the same scenarios after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 and emulated the solution using the same scenarios. Our simulation results are analyzed below:

Having emulated the Black Hole Attack, we noted that the packet loss is substantially increased in the ad-hoc network. In the readings, the tables of simulation results showed the difference between the number of packets lost in the network without and with a Black Hole Attack. This also showed that Black Hole Attack affects the overall connectivity of the network and the loss of data could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase. We could understand from the project that AODV network has normally in this network data 3.21% data loss and if a Black Hole Node is introducing loss is increased to 92.59. But after implementing our approach, there is vast decrease in packet drop and increase in throughput.

We emulated the Black Hole Attack in the Ad-hoc networks and investigated its effects. In our studies, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to give different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be decided. In our project, we try to eliminate the Black Hole effect in the network and detection of the Black Hole Node. In our works, we assume the black hole node is detected and tried to eliminate its effects. Our solution tries to eliminate the Black Hole effect by virtually increasing the distance vector between the attacker and the network. Additionally, we used TCP connection to be able to count the packets at sending and receiving nodes. In the TCP connection between nodes, the sending would be the end of the connection, since ACK packets do not reach the sending node. This is the solution for finding the BlackHole node. Finding the blackhole node with other connection oriented protocols could be another work as a future study.

IX. REFERENCES

1. https://en.wikipedia.org/
2. Charles E. Perkins. "Ad hoc Networking" , Pearson
3. P. Yau and C. J. Mitchell, "Security Vulnerabilities in Adhoc Network".
4. Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.
5. Web Tutorial for Adding Malicious node to AODV protocol http://elmurod.net/?p=196
6. H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.
7. https://www.youtube.com
8. K Fall and K. Varadha, The NS Manual, November 18, 2005, "htt ://www.isi.edu/nsnam/ns/doc/ "
9. Salim Hussain Sheikh. "Incorporation of Security Mechanism in AODV Routing Protocol to Eliminate the Effect of Black Hole Attack". October 2015
10. SEMIH DOKURER. A MASTER THESIS in Computer Engineering Atilim University "SIMULATION OF BLACK HOLE ATTACK IN WIRELESS AD-HOC NETWORKS". SEPTEMBER 2006

