IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Simulation of Black hole Nodes and Prevention Using IDS for MANET Reactive Routing Protocol AODV

Bhagyashree Thakur [*1] , Sharda Patel [2] , Ashok Verma [3] and Shivendu Dubey [4]

[1*,2,3,4]Dept. of CSE, Gyan Ganga Institute of Technology And Sciences, Jabalpur, M.P., India .

www.ijcaonline.org

Received: Nov /22 /2014 Revised: Nov/30/2014 Accepted: Dec/12/2014 Published: Dec/31/ 2014

Abstract- Mobile ad hoc networks (MANET) are widely used in that places where there is no available infrastructure. It is also called infrastructure less network. It is a collection of mobile nodes that dynamically form a temporary network without infrastructure. Each mobile node can move freely in any direction and changes their links to other devices frequently. In MANET different types of routing protocols have been recommended. Ad hoc On demand Distance Vector (AODV) is one of the most suitable routing protocol for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. In this paper, we have surveyed and compare the existing solutions to multiple black hole attacks on AODV protocol and their drawbacks.

Keywords— MANET, AODV, DRS, OLSR, DSDV

I. INTRODUCTION

The study of MANET has gained lots of interest of researchers. A Mobile ad hoc network as the name suggest, is self-configurable network of wireless. MANET is a collection of infrastructure less nodes which cooperates with each other to form temporary network. It consists of a collection of wireless mobile nodes that have capability to communicate with each other without the use of network infrastructure or any centralized administration. The nodes in ad hoc networks act as a host as well as router to forward the data packets. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations. Due to the inherent characteristics like dynamic topology and lack of a centralized management security, MANETs are vulnerable to several kinds of attacks like black hole attack, worm hole, denial of services Routing table overflow, impersonation, information disclosure etc.

II. ROUTING IN MANET

In MANETs nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

A. Reactive (On-Demand) Routing Protocol:

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source.

The two kinds of protocols are there in it AODV (Ad hoc On Demand Distance Vector Protocol), DSR (Dynamic source routing).

B. Proactive (Table Driven) Routing Protocol:

This protocol is also called as table driven protocol because routing information of nodes is exchanged, Periodically and accordingly the routing table is maintained, even when there is no communication. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. [6]

The two main kind of proactive protocols are Optimized link state routing (OLSR) protocol and Destination sequenced distance vector routing (DSDV) protocol.

C. Hybrid Routing Protocol:

This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and Temporally ordered Routing protocol (TORA).

III. RELATED WORK

A. Modified Routing Table:

[15]The solution involves two additional changes in the AODV protocol. First change is the addition of two

Corresponding Author: Bhagyashree Thakur parameters in the routing table. of each node in the network. These parameters are DATA_PCK_SENT and DATA_PCK_REC. DATA_PCK_SENT will count the total number of data packets sent to its next hop node, whereas, DATA_PCK_REC will count the data packets received from the next hop node. Secondly, an additional routing table known as Routing Information Table (RIT) is to be maintained at source node.

The purpose behind these two modifications is to increase the performance of AODV and eliminate the problem of Black Hole attack in MANET. The addition of RIT at source helps the source node to check the reliability of the intermediate node and then forwarding data to this node.

B. Improved Aodv Routing Protocol:

[6] It is an enhanced version of AODV and is hybrid in nature. IAODV mainly integrates two features: Multipath and Path accumulation .

Multipath: Multipath AODV reduces the route discovery frequency as compared to single path AODV. It finds multiple paths between a source and a destination in a route discovery process. Single path AODV initiates a new route discovery when it detects one path failure to the destination, whereas in multipath it creates a fresh route in case all the existing routes fail or expire. It also reduces the number of similar routes between source and destination nodes. A path with most similar nodes has a higher probability to create common links.

Path accumulation: Path accumulation feature enables us to append all discovered paths between source and destination nodes to the control messages as shown in figure 3(a). Hence, at any intermediate node the route request (RREQ) packet contains a list of all nodes traversed. Each node receiving these control messages updates its routing table. It adds paths to each node contained in these messages.

C. MAC Based:

[4] A solution for Black hole attack detection and prevention is proposed that uses the one-way-hash function H to generate MAC for RREP packet.

A Message Authentication Code (MAC) is a small part of information, which is used to authenticate and to provide integrity on the message. Cryptographic Hash Function is the only possible way to generate MACs. A MAC algorithm, accepts a variable length message as input, and outputs a fixed length MAC, also known as tag.

In cryptography, a keyed-hash message authentication code (HMAC) is a unique method for generating a MAC. It uses a cryptographic hash function with a mixture of secret cryptographic key. There are so many cryptographic hash function, such as Message-Digest algorithm (MD5) or Secure Hash Algorithm (SHA-1), they can be used in the generation of an HMAC; the resulting MAC algorithm is known as HMAC-MD5 or HMAC-SHA1 respectively.

D. Fidelity Table:

[9] A better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node’s level will be incremented. If no acknowledgement is received, the intermediate node’s level will be decremented.

E. DPRAODV (Detection,Prevention and Reactive AODV) Scheme:

[13] In this paper authors proposed have proposed the method DPRAODV .In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet.

F. Trust Value:

[14] The solution that we have proposed here is that we develop black hole AODV which allows some degree of node maliciousness to give an motivation to selfish nodes to state its malicious behavior to its neighbors which decreases searching time of misbehaving nodes. In proposed model the trust among nodes is represented by trust score. The trust calculation is based on packets loss rate if data packet is successfully transmitted then node trust value is incremented by 1, otherwise it becomes zero.

IV. AODV ROUTING SCHEME

The Ad-hoc On-Demand Distance Vector (AODV) is a reactive routing protocol designed to have intention for use in

mobile ad hoc networks. It finds a route to a destination when a node likes to transfer a packet to that destination. Route discovery process is based on the route information is stored in all intermediate nodes along the route in the form of route table entries. Every node has routing table, it has the fields like destination, next hop, number of hops, destination sequence number, active number of hops, destination sequence number, active neighbors and lifetime respectively. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are used to find the freshness of routes towards the destination.
The format of RREQ and RREP packets are in Fig 1(a) and 1(b) respectively.[8]

Scr_ Address	Scr_ Sequence	Broad cast_id	Dest_ Address	Dest_ Sequence	Hop Count

Fig: 1(a). AODV RREQ Field

Scr_ Address	Dest_ Address	Dest_ Sequence	Hop Count	Life Time

Fig: 1(b). AODV RREP Field

The given Fig 2(a) and 2(b) shows the propagation of the RREQ packets to all the neighbouring nodes, and the path of RREP packet towards the source respectively.

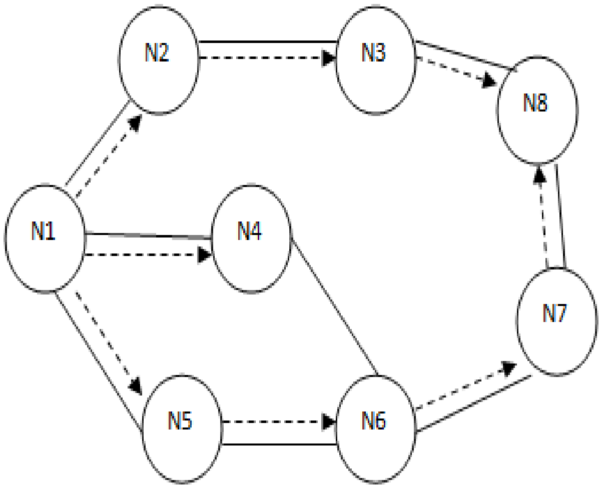

Fig: 2(a). Propagation of RREQ

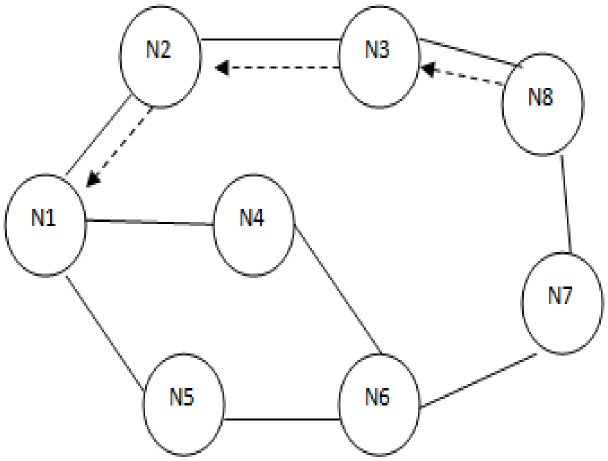

Fig: 2(b). The Path of RREP

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains source address along with request ID is incremented each time the source node sends a new RREQ and identifies it uniquely. On receiving a RREQ packet, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters the new RREQ packet will be discarded Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP packet: once a RREP packet is received, the route is established . A source node may receive multiple RREP packets with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information. While transmitting RREQ packets through the network, each node notes the reverse path to the source. When the destination node is found the RREp packet will travel along this path (the reverse path to the source[2].

Recently, most research on ad-hoc routing protocols, has been assumed trusted environment but, many usages of ad-hoc network run in untrusted situations. Therefore, most ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network.

V. BLACK HOLE ATTACK ON AODV PROTOCOL

Black hole attack is a big problem in MANETs in which an intermediate node works as malicious and consumes data before reaching to the destination. Black hole attack works in two phases in first phase, it advertises that it has a fresh route to the destination to deliver data packets with intention to drop data packets. In second phase it drops data packets without forwarding it. In this whenever any intermediate node gets a RREQ it immediately generates a RREP with high destination sequence number and sends it to the initiator. (Source) source stops receiving RREP and starts sending data packet to that node which has sent RREP to the source there are two kind of black hole attack.[10]

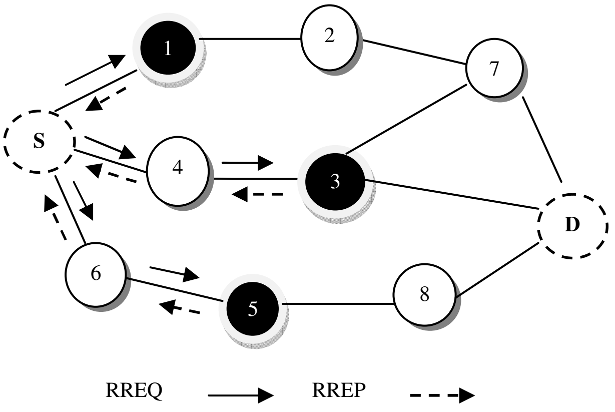

Fig: 3. Multiple Black Hole Nodes

In above figure, there are more than one black hole node i.e. 1,3 and 5 exists in the network at different places in order to drop the data packets.

VI. IMPLEMENTATION

A. NS2 SIMULATOR

We have use NS-2 (v-2.34), a network simulation tool to simulate the AODV routing protocol with attack and with the solution. It provides a good platform for MANET simulation. We simulate our model for 25 nodes. We have repeated the experiments by changing the number of Blackhole nodes to see the performance of network under attacks. The grid area is taken as 500 X 500 which is square.

Table I. Simulation Parameters

PARAMETERS	DEFINITION
Examined protocols	AODV
Simulation area (m x m)	500 x 500
Number Of Nodes	25
Traffic Type	CBR
Performance Parameter	Throughput, PDF, NRL, Drop, Routing Packets, Send Packets, Received Packets
No. of malicious node	1,2,3,4
Pause time	5 sec
Max Speed(M)	50

B. PROPOPSED METHOD

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. In our simulation module we apply IDS module that protect through the Black Hole behavior if Black Hole node in the range of IDS.

In our approach we have inbuilt Black hole module with AODV routing and IDS behavior module . Very first we attach Blackhole and IDS module in the NS-2 package and update the make file through following command:

```
blackhole/blackhole_logs.o blackhole/blackhole.o
blackhole/blackhole_rtable.o blackhole/b lackhole_rqueue.o

idsaodv/idsaodv_logs.o idsaodv/idsaodv_rtable.o
idsaodv/idsaodv_rqueue.o idsaodv/idsaodv.o \
```

After that we also add the agents of IDSAODV and BlackholeAODV and compile the internal module if new object file generated then we create TCL (tool command language script) for the scenario creation and create the MANET scenario, TCL invoke the new module Blackhole and IDS module and gives the behavior according to blackhole and IDS module. Then we create two different type of Output file name as .tr (trace file) and .nam (network animator file) through TCL script. Trace file contain each and every event information in particular discrete event of simulation and that file passes to awk (abstract window tool kit) and get the output in the form of routing overhead, throughput, Packet delivery ratio etc. Here we create three module names as AODV simple routing, IDS (intrusion detection and prevention system) module and Black hole module.

C. PERFORMANCE METRICS

Some important performance metrics can be evaluated:-

Normalized Routing Load — How many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets

Throughput — The ratio of the number of data packets sent and the number of data packets received.

Packet Delivery Ratio (Fraction)- It is calculated by dividing the number of packet received by destination through the number packet originated from source.

VII. RESULTS

Using outputs from awk script following graphs and results are generated.

A. Normalized Routing Load

Figure 4(a) show that AODV with Blackhole has a high routing overhead as compared to IDSAODV routing protocol .

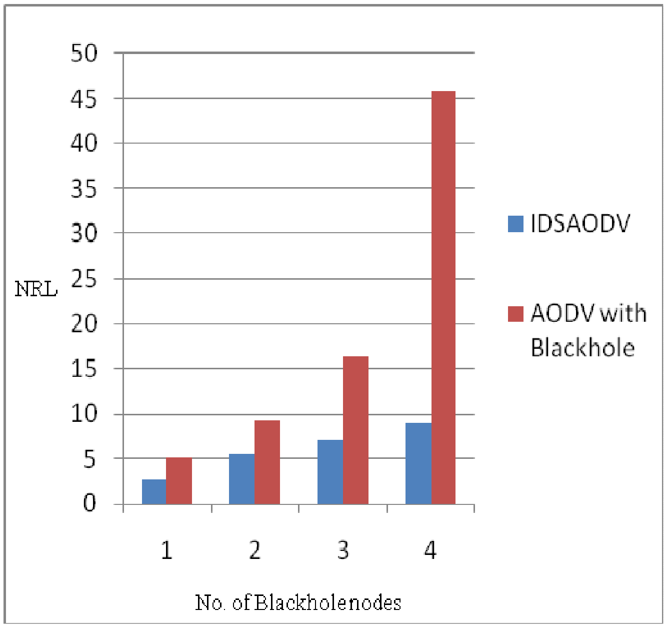

Fig. 4(a) Normalised Routing Load

B. Packet Delivery Ratio

Figure 4(b) show that pure IDSAODV has the Highest packet delivery fraction as compared to AODV with BLackhole.

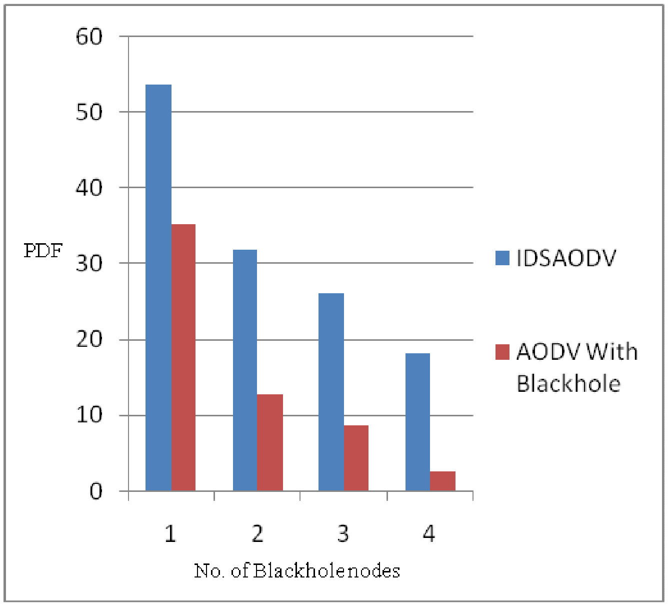

Fig. 4(b) Packet Delivery Ratio

C. Throughput

Figure 4(c) show that under blackhole attack the throughput of AODV is significantly lower as compared to IDSAODV .

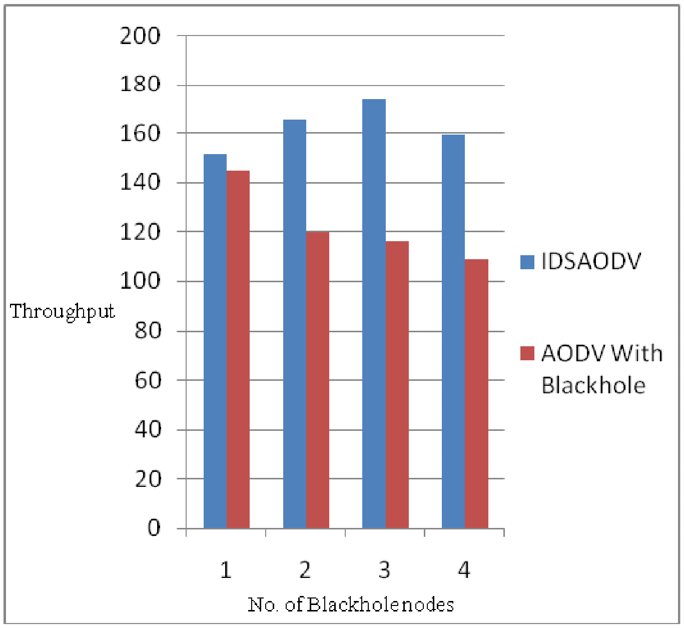

Fig.4(c) Throughput

D. Sending Packets

Figure 4(d) shows the number of packets send from source for AODV with Blackhole attack and IDSAODV under different scenario.

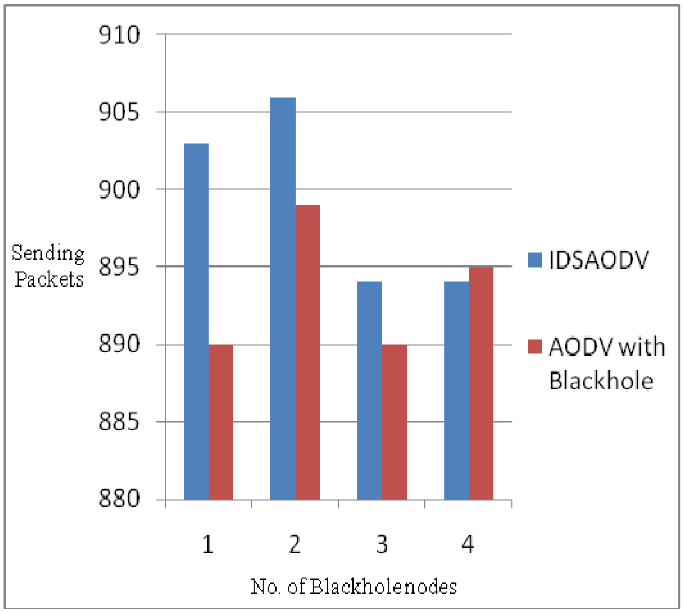

Fig.4(d) Sending Packets

E. RECEIVE PACKETS

Figure 4(e) shows the number of Packets Received by the nodes in accordance with the packets send which were shown in the above graph.

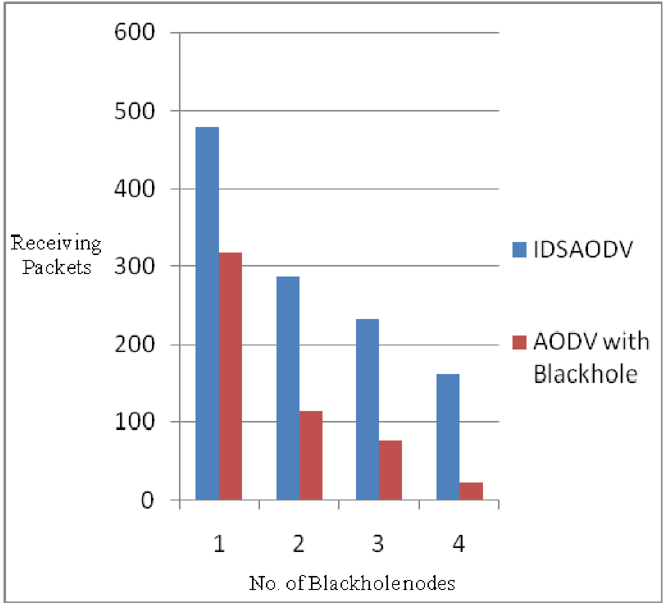

Fig.4(e) Receive Packets

F. Drop Packets

Figure 4(f) shows the number of packets drop in AODV protocol, with Blackhole attack and with the IDS solution.

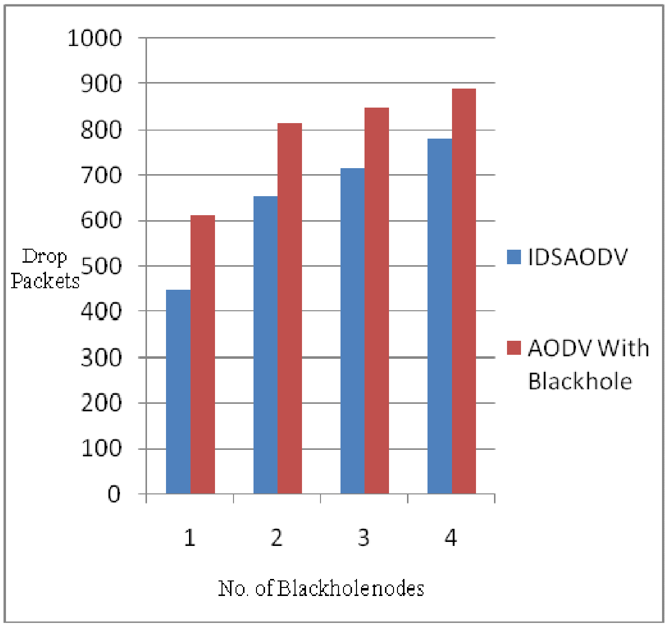

Fig. 4(f) Drop Packets

G. ROUTING PACKETS

Figure 4(g) show the number of packets route in the network with two protocols ie. AODV under attack and under solution in different scenerios.

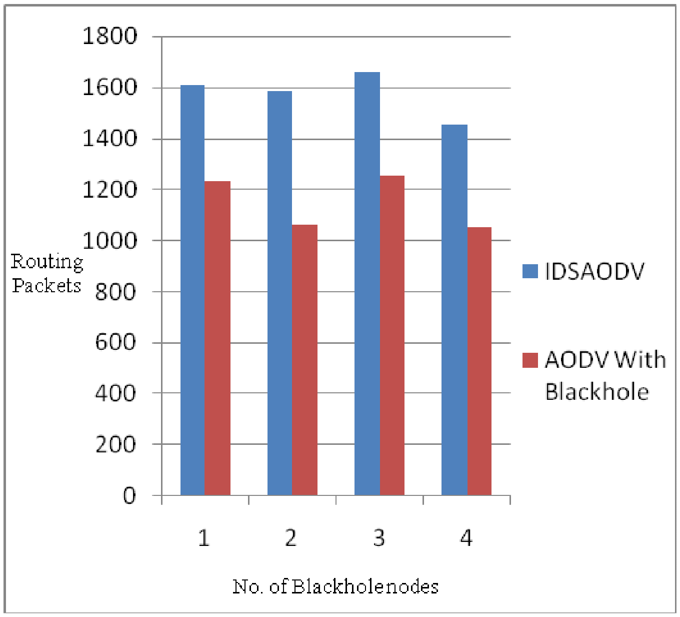

Fig.4(g) Routing Packets

H. NAM

NAM stands for Network Animator. It contains data for network topology. It starts with the command 'nam <nam-file>' where '<nam-file>' is the name of a nam trace file. At linux terminal command to run NAM is ./nam.

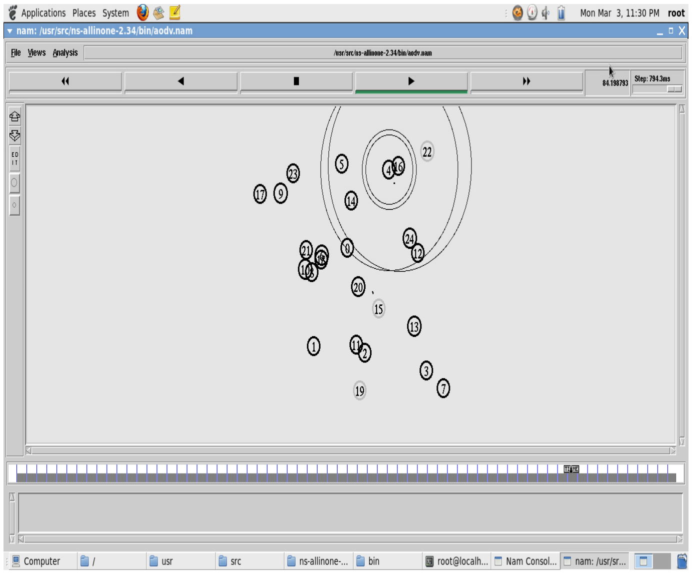

Fig. 4(h) Simulation Of BlackHole Attack in Network Animator

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have analyzed effect of the Black Hole attack in an AODV protocol of MANET. For this purpose, we have simulated an AODV protocol and its behavior in the presence of Black Hole nodes in NS-2. We have simulated four scenarios where each one has 25 nodes that use AODV protocol and also simulated the same scenarios after introducing Black Hole nodes into the network. Moreover, we have also simulated a solution that attempted to reduce the Black Hole attack effects in NS-2 We have also detected the Black Hole node by analyzing the .tr files.

In future this approach can be extended to other proactive and reactive routing protocols. We can also extend this research to secure routing protocols against other attacks such as Wormhole attack, Jellyfish attack etc.

REFERENCES

[1] Pooja Jaiswal, Dr. Rakesh Kumar “Prevention of Black Hole Attack in MANET”, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Y. Khamayseh, A. , Bader, W. Mardini and M. BaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks “International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; “A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS”, IEEE Wireless Communications • October 2007. PP: 85-90.

[4] Pooja Vinod Kumar Department of Computer Science and Applications”A Review on Detection of Blackhole Attack Techniques in MANET” Volume 4, Issue 4, April 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[5] “ Modified AODV Protocol against Black hole Attacks in MANET” by K. Lakshmi1, S.Manju Priya, A.Jeevarathinam, K.Rama, K.Thilagam

[6] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010

[7] Jaspal Kumar, M. Kulkarni, Panipat Institute of Engineering & Technology, India National Institute of Technology, Karnataka, India “Effect of Black Hole Attack on MANET Routing Protocols” I. J. Computer Network and Information Security, 2013, 5, 64-72 Published Online April 2013 in MECS

[8] C. Kim, E. Talipov and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks," Pro- ceeding from EUC'06: The 2006 International Confer- ence on Emerging Directions in Embedded and Ubiqui- tous Computing, Seoul, 1-4 August 2006, pp. 522-531.

[9] Ravi KantvM.tech ScholarvABES EC, Ghaziabad” A Literature Survey on Black Hole Attacks on AODV Protocol in MANET” International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013

[10] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[11] K. Makki, N. Pissinou, and H. Huang, “Solutions to the black hole problem in mobile ad-hoc network,” 5th World Wireless Congress, pp.508–512, 2004.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[12] S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

[13] Bhoomika Patel Department of Information Technology, Parul Institute of Engineering & Technology, Limda,Vadodara, India.” A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,

[14] Nirali Modi, Vinit Kumar Gupta Department of computer engineering Hasmukh Goswami College of Engineering, Ahmedabad, India” Prevention Of Black hole Attack using AODV Routing Protocol in MANET” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,

[15] Neha Kaushik, M.Tech Student Ajay Dureja, Assistant Prof. PDM College of Engineering for Women, B’Garh” Performance Evaluation Of Modified Aodv Against Black Hole Attack In Manet” European Scientific Journal June 2013 edition vol.9, No.18