ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v4.i11.2017.126

IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

ANALYSIS OF BLACK HOLE ATTACK DURING ROUTE DISCOVERY PHASE OF AODV IN MANET

Lalit Kumar Tripathi [*1], Dr. Kanojia Sindhuben [2]
[*1, 2] Computer Science & Engineering, United Institute of Technology Naini Allahabad, India

Abstract:
MANET (Mobile ad hoc networks) is a collection of wireless mobile nodes dynamically forming an infrastructure less network. Several routing protocols are designed for routing of packets in MANET. One of them is AODV (Ad hoc on demand Distance Vector) protocol whose performance is better for higher mobile nodes. It is more vulnerable to black hole attack by the malicious node. Black hole attack is a network layer attack in MANET that tries to hamper the routing process. During route discovery phase it sends false reply to the nodes and dropped data packets. In this paper, first we have implemented black hole attack in AODV and then analyzed the impact of black hole attack under deferent metrics like throughput, packet delivery ratio and packet loss. Simulator NS-2.35 is used for implementation and result analysis.

Keywords: *AODV; Black hole Attack; MANET; NS-2.35.*

Cite This Article: Lalit Kumar Tripathi, and Dr. Kanojia Sindhuben. (2017). "ANALYSIS OF BLACK HOLE ATTACK DURING ROUTE DISCOVERY PHASE OF AODV IN MANET." *International Journal of Engineering Technologies and Management Research*, 4(11), 75-80. DOI: https://doi.org/10.29121/ijetmr.v4.i11.2017.126.

1. Introduction

MANET or mobile ad hoc network is the infrastructure less network. All the nodes in MANET act as a router to route the packet and does not require any external base station or access point to transfer data among nodes. Routing the packets are used by different routing protocols. Routing protocols in MANET are classified into three categories i.e., reactive, proactive and hybrid.

Security is the main concern because nodes in MANET are mobile [4]. Malicious nodes (unwanted node) try to enter in the network and degrade the performance of the network. AODV [1,2] is one of the most suitable routing protocol for MANET and it is more vulnerable to black hole attack [3] by the malicious nodes. In the black hole attack a malicious node absorb all data packets in itself. Malicious nodes dropping all the traffic in the network make use of the vulnerability of the root discovery packets of the on demand protocols such as AODV. In case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of effect is known as cooperative black hole attack. The paper is concerned about the implementation algorithm of black hole attack in AODV. Also working of AODV and Black

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117167

hole AODV is evaluated for various parameters such as throughput, end to end delay, and packet delivery ratio. Simulations are done in NS 2.35 tool [9].

2. AODV Overview

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks [1, 7]. AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time based states in each node: a routing-entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ. Route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

3. Implementation of Black Hole Attack

To implement black hole attack during route discovery phase of aodv protocol, some changes are made in *aodv.h* and *aodv.cc* file inside ns2.35 simulator [6,10]. Following are the steps to make changes:

Step1: In aodv.h file, declare a boolean variable malicious as shown below in the protected scope in the class AODV-

bool malicious;

Step2: In aodv.cc file, following changes are required:-

a) Initialize the malicious variable with a value "false". Declare it inside the constructor as shown below-

AODV::AODV (nsaddr_tid): Agent (PT_AODV)...

{

.....

Malicious = false;

}

b) Add the following statement to the aodv.cc file in the "if(argc==2)" statment.

```
if(strcmp(argv[1],"hacker")==0){
 malicious=true;
  returnTCL_OK;
}
```

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117167

c) Implement the behavior of the malicious node by setting the following code in the rt_resolve(Packet *p) function.

The malicious node will simply drop the packet and specify a reason for dropping as indicated below.

```
if(malicious==true){
  drop(p,DROP_RTR_ROUTE_LOOP);
}
```

Once done, recompile ns2 as given below command in terminal-

Make

Once the compilation is done, check the malicious behavior using the Tcl Script by setting any one node as malicious node. The command to set the malicious node is

$ns at 0.0 "[$n2 set ragent_] malicious"

4. Simulation Parameters and Metrics

Simulations are performed for analyzing the impact of implemented black hole attack on AODV and normal AODV [8]. NS-2.35 tool is used for performing the simulations. NS-2.35 is the simulation tool which provides the platform for the simulation of various routing protocols, multicast protocols and different topology over wireless or wired networks. Simulations are done to both AODV and black hole affected AODV for nodes 20, 40, 60, 80 and 100. Malicious nodes are used in three phase during black hole attack on AODV. In first phase only one malicious node is used on node_3. In second phase two malicious nodes are used on node_3 and node_6. In third phase three malicious nodes are used on node_3, node_6 and node_9. Simulation parameters and their values used during the simulations are mentioned below in table 1.

Table 1: Simulation Parameters

Protocol	AODV
No. of Nodes	20, 40, 60, 80, 100
No. of malicious nodes	1 (node_3), 2 (node_3, node_6) and 3 (node_3, node_6, node_9)
MAC	IEEE 802.11
Propagation	Two Way Ground
Traffic Connection	CBR over UDP on 5 nodes
Size of Packet	512 bytes
Mobility	Random Way Point
Speed	Minimum=0 to maximum=10
Simulation Area	1000x1000 (m x m)
Simulation Time	200 sec

The following some metrics have used for analyzing the impact of black hole attack [5] on AODV.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117167

Packet Delivery Ratio: PDF is defined as the ratio of all the data packets that are received by the destination node to the total number of packets being generated by the CBR source node.

Throughput: It is the rate at which data packets are transmitted per unit time in the network. It is measured in kbps or bps.

Total Packet Dropped: To evaluate dropped packets we count how many packets are sent by the source nodes and how many of them reached the Destination nodes.

5. Results Analysis with Graphs

Simulations are done using the parameters mentioned above for AODV and black hole attack AODV with multiple malicious nodes. Three different metrices are used to analyze the results as shown in graph.

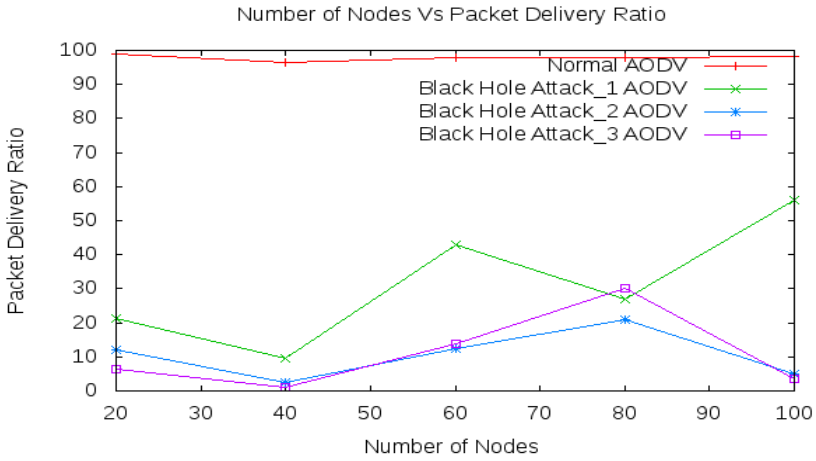

Figure 2: Packet delivery ratio of normal AODV and black hole attack AODV

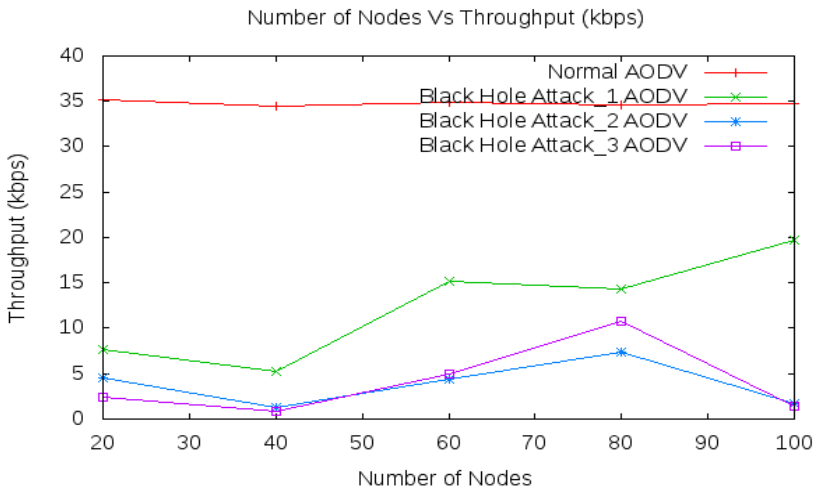

Figure 3: Throughput of normal AODV and black hole attack AODV

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117167

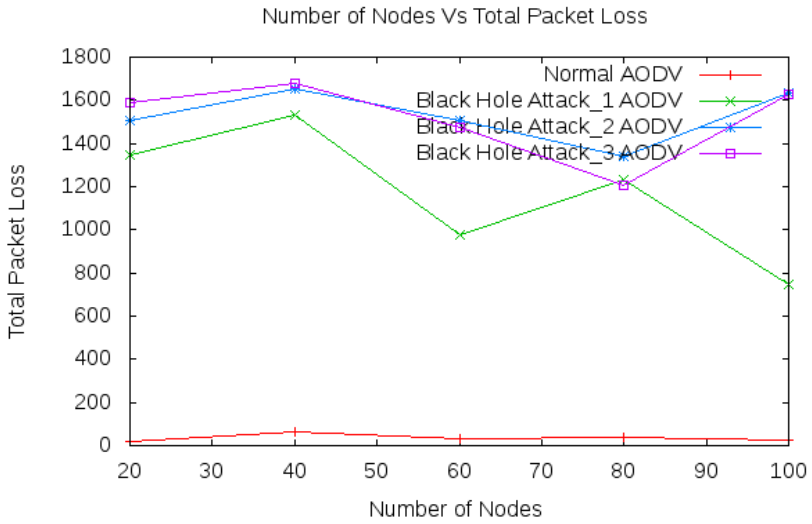

Figure 4: Total packet loss of normal AODV and black hole attack AODV.

From the above graphs for AODV and black hole attack AODV with multiple malicious node it is observed that with the impact of black hole attack the performance of normal AODV is affected. Figure 2 shows the comparison between packet delivery ratio of normal AODV and black hole attack AODV. It is observed that PDR for black hole attack AODV is less than that of normal AODV. In figure 3 Throughput of AODV and black hole attack AODV is compared. From the graph it is seen clearly that with the rise in number of nodes the throughput for normal AODV also rises where for black hole attack AODV it falls. Total packet loss of normal AODV and black hole attack AODV is being compared in figure 4. It is found that the packet loss for the normal AODV is comparatively less whereas for black hole attack AODV it rises steeply when the number of nodes increase.

6. Conclusion

In this paper, we have implemented and analyzed the effect of black hole attack in AODV protocol. Simulations are performed on three metrics viz. packet delivery ratio, throughput and total packet loss for normal AODV and AODV affected by black hole.

Traffic and mobility scenario was same for both normal AODV and to maintain the uniformity. Based on the above performance comparisons, AODV under the black hole effect packets Dropped rises whereas throughput and PDR falls compare normal AODV. Finally we conclude that black hole attacks affect the AODV routing protocol negatively.

Acknowledgment

I would like to extend my sincere gratitude to my guide Dr. Kanojia Sindhuben, for allowing me to work on this project. Without her help and support this project would not have been possible.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1117167

References

[1] C. E. Perkins, "The Ad Hoc On-Demand Distance-Vector Protocol (AODV)" Ad Hoc Networking, Addison-Wesley, pp. 173–219, 2001.
[2] C. Perkins, E Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing", RFC 3561, July 2003.
[3] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Humancentric Computing and Information Sciences 2011, 1:4.
[4] Burbank JL, Chimento PF, Haberman BK, Kasch WT "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology". IEEE Communication Magazine 44(11):39–45, 2009.
[5] Ei Ei Khin and Thandar Phyu, "IMPACT OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOL" International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.
[6] Sushil Kumar, Deepak Singh Rana and 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.
[7] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
[8] Semih Dokurer, Y.M. Erten, Can Erkin Acar, "Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148-153, 2007.
[9] http://www.isi.edu/nsnam/ns/
[10] http://mohittahiliani.blogspot.in/

*Corresponding author.
E-mail address: lalittripathi11 @gmail.com