IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. III (Sep.- Oct. 2017), PP 06-10
www.iosrjournals.org

Tracing down Black hole attack in MANETS

Dr. G. Krishna Kishore[1], K. Jahnavi[2], D. Suresh Babu[3]

[1]*(Professor, Computer Science Department, VR Siddhartha Engineering College, Vijayawada, India)*
[2] *(Student, Computer Science Department, VR Siddhartha Engineering College, Vijayawada, India)*
[3]*(Asst .professor, Computer Science Department, VR Siddhartha Engineering College, Vijayawada, India)*

Abstract: *A mobile ad-hoc network (MANET) is a union of numerous connectionless mobile nodes which transmit data through wireless channels, in the absence of any stable infrastructure. Both genuine and malevolent nodes can ingress the network. So MANETS are predominantly liable to many assaults or attacks. The dropping of data packet while transmitting from source to goal is one of the critical problems in MANETS. There are many factors by which this data packet droppings is caused. One foremost cause for this packet loss is black hole attack. In black hole assault a malevolent node publicize itself as it is having briefest way from source to the goal nodes during routing location process and switch the data towards it and then drops that data instead of reaching actual destination. Here we concentrate on tracing of Black hole assault in Ad Hoc On-Demand Distance Vector (AODV) protocol. The work is carried on NS-3 (Network Simulator).*

Keywords**:** *AODV, Black hole attack, MANET, NS3.*

Date of Submission: 15-09-2017 Date of acceptance: 28-09-2017

I. Introduction

In MANETS when node requires exchanging information to other node, this exchanging is done by using the middle nodes, hence seeking and constructing way from source to goal is a vital errand in MANET. Routing is an essential segment in MANETs and it had numerous protocols. On-request Distance Vector (AODV) is the privileged one for route convention in MANETS; moreover this is endangered to black hole assault.

1.1 Routing protocols in MANETS

The procedure of information interchange from one node to the other node in MANETS is called routing in network. These are split into three categories: Proactive, Reactive and Hybrid routing protocols.

1.2 Ad Hoc On-Demand Distance Vector (AODV) Protocol

AODV comes under reactive routing protocol. It is utilized for looking and constructing routes between the source and goal nodes. This route discovery process takes place only when it is needed. It lessen the quantity of communication by generating paths based on interest [3]. In AODV protocols there are three sorts of messages are utilized for path recognise purpose. They are Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. Route request message is utilized to detect the path to the goal node, and when destination is detected it sends the route reply message. Route error message is broadcasted to whole nodes whenever the breakage in the link is found.

1.3 Black Hole Attack

Black hole attack is a sort of assault or attack where a noxious node deliver a phony reply packet to the source node that had started the path discovery process, to present itself as a goal node to the real goal or destination node. In this situation the source node will send the greater part of its information to the noxious node [1] .This noxious node then retains the packets send by source node and drops them completely or partially sometimes. As a result the information never reaches the goal node.

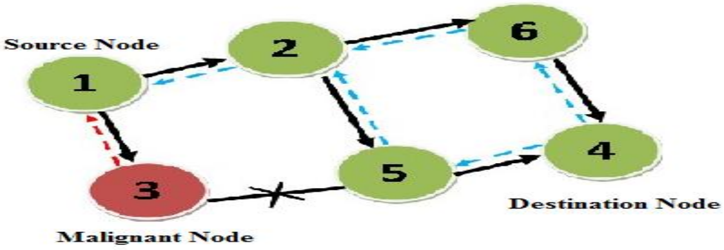


Fig 1. Black hole attack

In figure 1 the source node is 1 and destination node is 4 and the malignant node is 3 which function as official node. When this source node 1 transmit the route request packets to its neighbouring nodes then malignant node 3 reply first than all others nodes and steal the data from this source node 1 and then drop the packet instead of the packet reaching the goal or destination node.

Black hole attack in MANETS is classified into two types:

1.3.1 Internal Black hole attack

In internal black hole attack, the malevolent node is available in middle path of source and destination nodes. When this malevolent node gets the chance, it behaves like an official node.

1.3.2 External Black hole attack

In external black hole attack, the malevolent node is existed exterior of the network. When it gets chance it creates cognition in the network.

II. Related Work

To identify black hole in MANETS many researches were done by many researchers. [5] proposed a result in which in route request message two destination internet protocol address are given. One is genuine destination internet protocol address and second is fake internet protocol address. The sake of adding two destination IP addresses is that only malignant node will send reply for both IP addresses, and genuine node answer only for desired valid IP address. If a node replies for two destination IP addresses then it is traced as black hole node.

A safe knowledge algorithm to perceive black hole attack [6]. In this algorithm a promiscuous mode is used to ensure data delivery to receiver node. Here two tables namely fm table to grip the data about packets that are recently transmitted and rm table to hole the neighbouring node information is constructed. In this AODV is adjusted so all nodes in the network listen to their neighbour nodes promiscuously and then compare the neighbour node information in its fm and rm table. If any entries in the table has fm not equal to rm and threshold value is reached then modification attack otherwise trusted node. If rm and threshold value is reached then Black hole attack.

The aggressor node by using clock based location approach[7]. In this strategy each node specify a trust value for its neighbour node and install a timer with each packet, if that value falls under a threshold value for any node, then that node is put in the black list table.

Number of source or neighbour node who has reply the first route reply or not[8]. Firstly the initial respond comes from the attacker node that consisting the highest destination sequence number and this sequence number data is kept as initial entree in route request table. Then collate the initial goal sequence number with source node sequence number, if more differences occurs among them, then it is from the mischievous node, instantly detach its entry from the route request table.

III. Proposed Solution

First source node sends a route request message to the adjoining nodes to locate the exact goal node. On receiving the reply from those nodes, source node extracts that data and checks the outcome which is obtained from them. If the outcome is correct, then it begins a path to the destination and sends the data. If the outcome is not correct an additional route to the neighbour nodes is send to examine whether the route from the intermediate node to the destination node exists or not. At the same time, it sends an alarm message to the total network to remove the noxious node. Hence we evade this black hole problem.

In this method we identified the black hole attack in AODV routing and the execution is shown using network simulator (Ns-3). The results are executed in five different cases.

- Case 1: hidden black hole attack with 100% packet loss is shown.
- Case 2: exposed black hole attack with 100% packet loss is displayed.
- Case 3: active black hole attack with certain % packet loss is exhibited.
- Case 4: black hole attack with zero mobility is shown with no packet loss.
- Case 5: black hole attack with mobility is shown with certain packet loss.

Algorithm:

- *Step 1*: In Enhanced-AODV route request message includes fields like source internet protocol address, destination internet protocol address, hop count, communication ID, source and destination sequence numbers to individually distinguish this route request message.
- *Step 2*: When the destination node acquire the first route request message, it produces turn around route request (TA-RREQ) message and convey it to adjacent nodes that are present inside the transmission range.

- *Step 3*: In Enhanced-AODV turn around route request message contains fields like communicate ID, destination internet protocol address, destination sequence number, source internet protocol address, and hop count.
- *Step 4*: When broadcasted TA-RREQ packet reaches to center node, it will check for duplicate messages.
- *Step 5*: If it already got the alike message, the message is dropped, if not send the message to consequent nodes.
- *Step 6*: When the source node gets initial TA-RREQ message, then it begin to send the packet.
- *Step 7*: Late arrived TA-RREQs are kept for additional utilize.
- *Step 8*: The alternate direction is utilized when principal route breaks during the process establishment.

IV. Simulation Environment

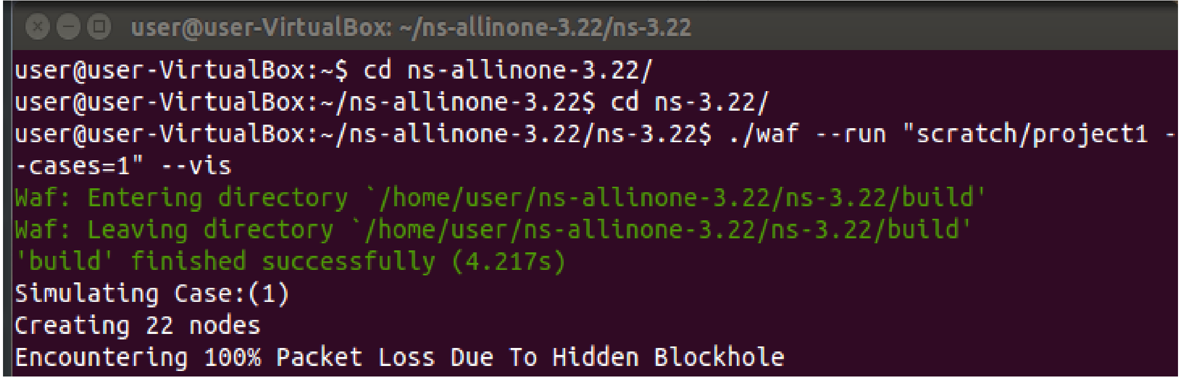
The identification of Black hole attack is done in NS-3 simulator.

Table1: Simulation Setup Parameters

Parameters	**Values**
Simulator	NS-3
Number of nodes	22
Routing protocol	AODV Routing protocol
Simulation time	35 sec
Network structure	Grid structure

4.1 Output Screens

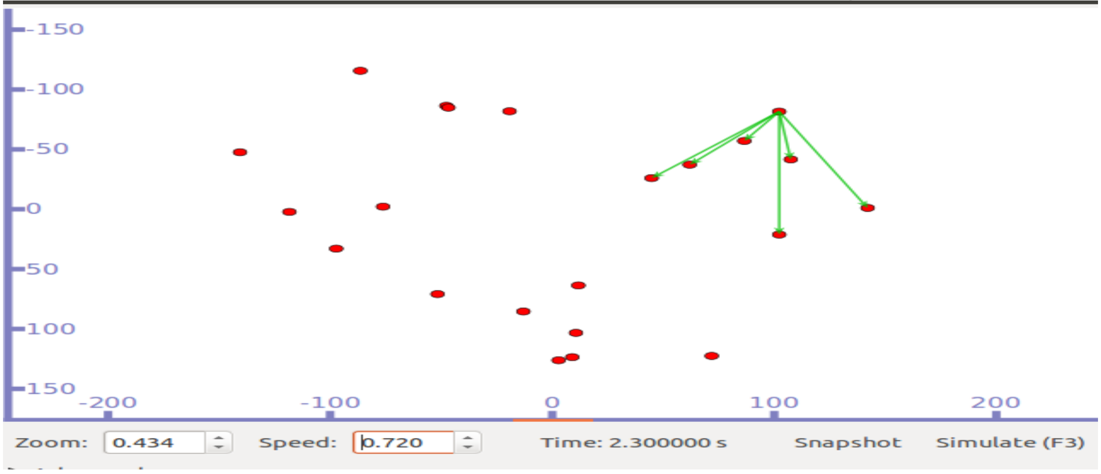
Case 1: In case 1 hidden black hole with 100% packet loss is displayed.



```
user@user-VirtualBox:~$ cd ns-allinone-3.22/
user@user-VirtualBox:~/ns-allinone-3.22$ cd ns-3.22/
user@user-VirtualBox:~/ns-allinone-3.22/ns-3.22$ ./waf --run "scratch/project1 -
-cases=1" --vis
Waf: Entering directory `/home/user/ns-allinone-3.22/ns-3.22/build'
Waf: Leaving directory `/home/user/ns-allinone-3.22/ns-3.22/build'
'build' finished successfully (4.217s)
Simulating Case:(1)
Creating 22 nodes
Encountering 100% Packet Loss Due To Hidden Blockhole
```

Fig 2. output for hidden Black hole in terminal

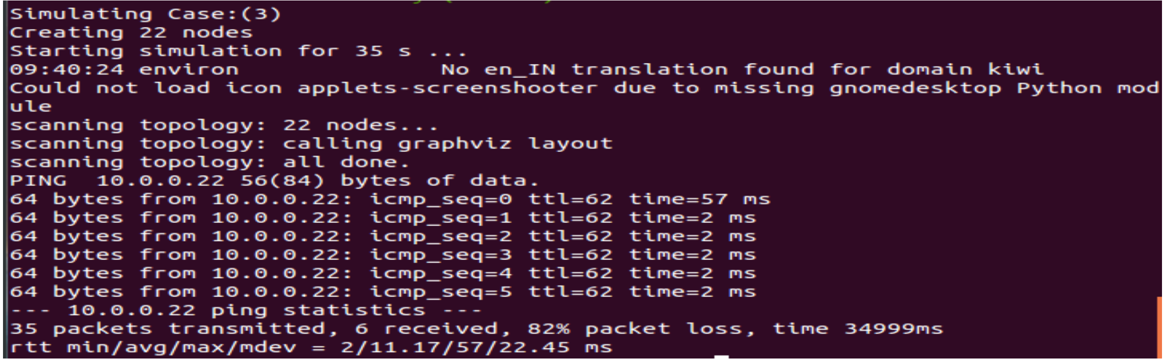
Case2: In case 2 exposed passive black hole with 100% packet loss is shown creating traffic in network.



Zoom: 0.434 Speed: 0.720 Time: 2.300000 s

Fig 3. Output for exposed Black hole

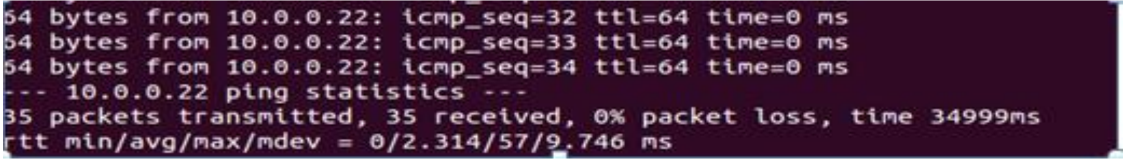
Case 3**:** In case 3 hidden black hole with certain % packet loss in terminal.



```
Simulating Case:(3)
Creating 22 nodes
Starting simulation for 35 s ...
09:40:24 environ              No en_IN translation found for domain kiwi
Could not load icon applets-screenshooter due to missing gnomedesktop Python mod
ule
scanning topology: 22 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
PING  10.0.0.22 56(84) bytes of data.
64 bytes from 10.0.0.22: icmp_seq=0 ttl=62 time=57 ms
64 bytes from 10.0.0.22: icmp_seq=1 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=2 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=3 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=4 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=5 ttl=62 time=2 ms
--- 10.0.0.22 ping statistics ---
35 packets transmitted, 6 received, 82% packet loss, time 34999ms
rtt min/avg/max/mdev = 2/11.17/57/22.45 ms
```

Fig 4. Output for hidden Black hole

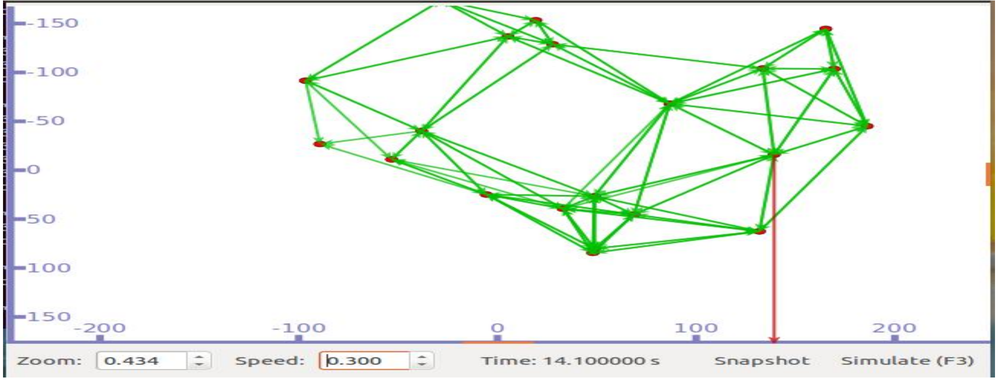
Case 4: In case 4 black hole with zero mobility and with no packet loss is shown in terminal



```
64 bytes from 10.0.0.22: icmp_seq=32 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=33 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=34 ttl=64 time=0 ms
--- 10.0.0.22 ping statistics ---
35 packets transmitted, 35 received, 0% packet loss, time 34999ms
rtt min/avg/max/mdev = 0/2.314/57/9.746 ms
```

Fig 5. Output for Black hole with zero mobility and no packet loss

Case5: Output screen shot for case 5 showing packet dropping in simulator



Zoom: 0.434 Speed: 0.300 Time: 14.100000 s

Fig 6. Output showing the packet dropping

The arrow red line in the above figure indicates packet dropping from network due to the existing of Black hole node.

V. Result Analysis

Comparison results between AODV and Enhanced AODV

5.1 Packet Loss: This packet loss tells about the amount of packets that are transfered from source node but failed to reach the destination node.

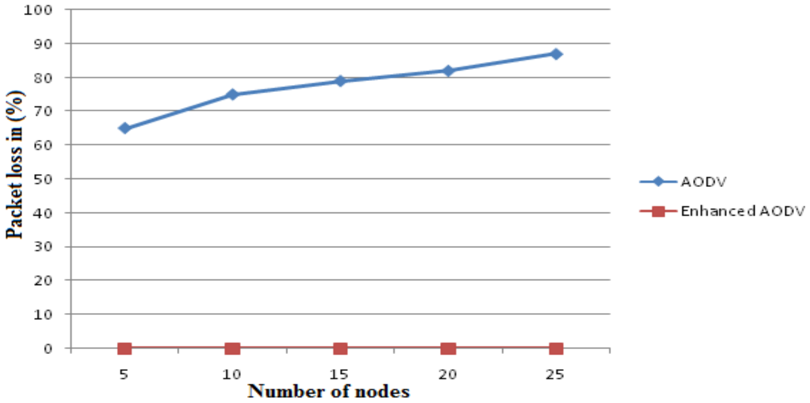


Fig 7. Packet Loss

The above graph show the information about the percentage of packets that are dropped from the network during the exchange of data between the source node and the destination node.

5.2 Throughput: This throughput describes about the amount of bits transmited or received per second in the network.

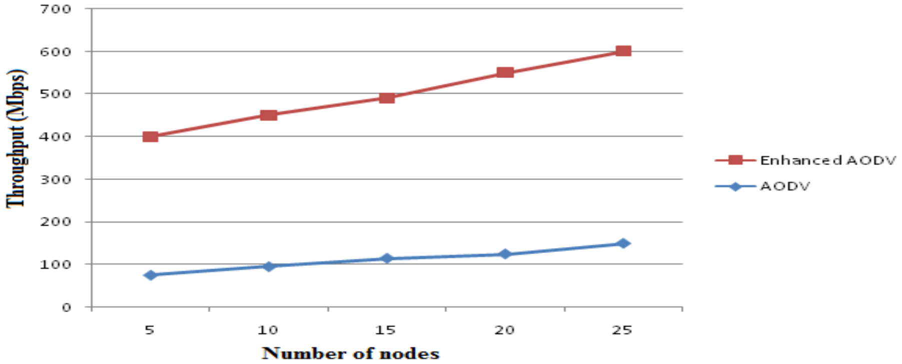


Fig 8. Throughput

The above graph show the throughput with respect to increasing nodes in both AODV and Enhanced AODV.

VI. Conclusion And Future Work

In MANETS routing protocols plays a very paramount role because overall performance of network depends on the pattern of routing protocols. Black Hole Attack is a main security threat which infects the presentation of the AODV protocol in MANETS. A number of researches are conducted by using various approaches to prevent black hole problem in MANETS using Ns-2. Here we implemented a new work to trace black hole and simulation is carried using Ns-3. This entire implementation reveals that our new method when applied on AODV protocol gives better results.

In future we try to apply this approach for the prevention of various attacks in MANETS using Ns-3 simulator and also we can apply this method by increasing number of attacker nodes and also by increasing number of nodes in the network.

References

[1]. Irshad ullah, Shoaib ur rehman, *Analysis of Black hole attack on MANETs Using distinctive MANET routing protocols* – 2010

[2]. Sonika Malik, Indu Kashyap, *Identif'ying, Avoidance and Performance Assessment of Black Hole Attack on AODV Protocol in MANET* - International Journal of Computer Applications IJCA – 2014

[3]. T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj, *Removal of Selective Black Hole Attack in MANET by AODV Protocol* - International Journal of Innovative Research in Science, Engineering and Technology - 2014

[4]. Dr.S.Tamilarasan, *Securing AODV Routing Protocol from Black Hole Attack* - International Journal of Computer Science and Telecommunications - 2012

[5]. Nidhi Tiwari, - *Detection of Black Hole Attack using Control Packets in AODV Protocol for MANET* - International Journal of Computer Applications -2015

[6]. Siddiqua, Ayesha, Kotari Sridevi, *Preventing black hole attacks in MANETs using secure knowledge algorithm*, Signal Processing And Communication Engineering Systems, 2015 International Conference - 2015.

[7]. Choudhary, Nidhi, and Lokesh Tharani. *Preventing black hole attack in AODV using timer-based detection mechanism*, Signal processing and communication engineering systems, 2015 international conference - 2015.

[8]. Lalit Himral, *Keeping AODV Routing Protocol from Black Hole Attack*, International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[9]. Vasanthavalli.S, Dr.S.Thenappan, *Peruse Of Black Hole Attack and Prevention Using AODV on MANET*, International Journal of Computer Applications – 2014

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Dr. G. Krishna Kishore. “Tracing down Black hole attack in MANETS.” IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 06–10.