International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Performance Analysis of Black Hole Attack with AODV using Different No. of Nodes in VANET

Bharti[1], D. P. Dwivedi[2]

[1]M.Tech. Student VIET, G.B. Nagar

[2] Dept. of Computer Science VIET, G.B. Nagar

Abstract: ***Vehicle Ad-hoc Network is vulnerable to several attacks. One of the main attack is the black hole attack which absorbs all the data packets in the network. In this paper, we have analysed the performance of VANET in presence of BLACK HOLE node by using AODV routing protocol.The main parameter considered are throughput, end-to-end delay and packet-drop-ratio.These parameter are compared for AODV routing protocol both using black hole attack and without black hole attack. The simulation setup comprises of 10,20,30,40 Vehicular nodesmoving with constant speed. Simulation is carried using Network Simulation (NS2)2.35.***

Keywords: VANET- Vehicle Ad-hoc Network, AODV –Ad-hoc On Demand Distance VectorRouting, RREQ-Route Request, RREP – Route Reply, Black hole Attack

1. Introduction

VANET-VANET is a new form of MANET(Mobile Ad-hoc Network) which consists of number of vehicles with the capability of communicating with each other without a fixed infrastructure. So VANET is has a highly dynamic topology as compared to MANET. The Black Hole Attack is one of the security threats in VANETs. In Black Hole Attack, when there is any route request, one malicious node send the reply to having the shortest path to the destination node or to the packet it wants to intercept. When the malicious node receives an RREQ message, then malicious node immediately sends a false RREP massage over its route, which has high sequenceNo. So, malicious node will always have the availability in replying to theroute request and thus it cheat with the source node. The malicious node reply to the requesting node before reply from the actual node; hence a false and malicious path created. And all data send to this false route so the data Packet lost.

In this figure(1), „A" wants to send the data to node „D" initiate the route search process. If Node „F" is a malicious node then it will claim that it has active route to the destination as soon as it receives RREQ packets and sends the reply to Node „A" before any other sends reply for the shortest path. So Node „A" think it is the active route and discovery is complete and sends the data packets to node „C" and ignore all other replies[1]. So all data packet will be lost or consumed.

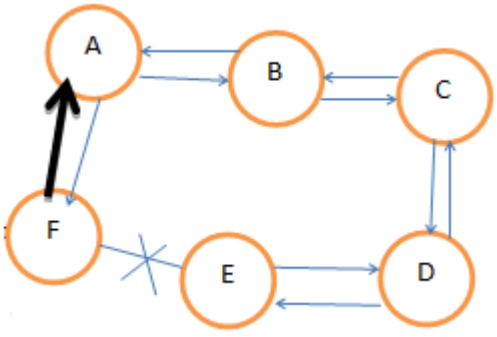

Figure 1: Black Hole Attack

2. Attack in the VANET

To get the better protection from attackers we must have the knowledge about the attacks in VANET against security requirements [2].

- ***Denial of Services*:**In this attack Attackers prevents the legitimate user to use the services from the victim node. DoS attacks can be carried out in many ways:
- ***Jamming*:** In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is **jam.**
- ***Distributed DoS Attack:***This is the another form DoS Attack. In this attack, multiple attackers attack the victim node and prevents the legimate user from accessing the services.
- ***Routing Attack:***Routing attacks are the attacks which exploits the vulnerability of network layer routing protocol. In this type of attack the attackers either drop the packet or disturbs the routing process of the network. Following are the most common routing attack in VANET:
- *Black hole attack*: In this type of attack the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with showing itself as a fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet. It has some cheraistics:
  Route Blocking: With this malicious node does not forward the data to the other node and send the false RREP to the requested node.
  Packet Dropping: In the packet drooping this node does not forward the data to the other node in the route but silently drop the data packet.
  In this we are using a ***DROP_MAL() function*** *which drops the packet in AODV which is the reason of the Black hole attack. When Packet Drops More then Throughput reduced and packet drop ratio increased.*
- *Worm hole attack:*An adversary receives the packet at one point in the network, tunnels them to another point in the

Licensed Under Creative Commons Attribution CC BY

network and then replays them into the network from that point. This tunnel between two adversaries are called **wormhole**. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunnelled packet arrive sooner than other packet transmitted over a normal multi-hop route.

- *Gray hole attack:* This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively.

3. Routing Protocol

1) AODV Routing Protocol

AODV is an On Demand Routing Protocol. They are not maintained periodically but routing tables are created only when required. In AODV the source node and the intermediate nodes store the next hop for the each flow for data packet transmission. The AODV adds a advantage over Table driven Routing Protocol in which every node has to keep up to date routing tables. This routing protocol is used for finding a path to destination in ad-hoc-network. AODV has the three messages RREQ(route request), RREP(Route Reply), RErr (Route Error)[7]. When any node needs path for destination , RREQ is send to all neighbouring nodes. If any node has path that node sends a RREP to source node otherwise sends the RREQ to the other nodes, on receiving RREP source node send data packet to the node which has path for destination. This process continuous until the packet is received by the destination[3].

4. Simulation Tool and Setup

Simulation is performed using simulator NS2 2.35. It is best simulator in ad-hoc-network[4][6].At terminal, it produces NAM (network Animator).

The aim of this paper is to determine measurement throughput, end-to-end delay and Packet drop ratio on diff-diff. nodes 10, 20, 30, 40 with black hole and without black hole node.

Table 1: Simulation parameters

Simulator	NS-2(2.35)
Simulation time	1000 sec
No.of nodes	10,20,30,40
Routing Protocol	AODV
Movement Model	ManhattanGrid
No. of Black hole	1
Mac Layer	802.11
Traffic type	CBR

5. Performance Parameters

Metrics selected to evaluate performance of routing protocol AODV are throughput, packet drop ratio.

- *Throughput:* It is the ratio of total no. of packets received to total no. of packets send by the sender. Throughput is measured in terms of bits per second.[5].
- *End-to-end delay:* End-to end delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in the data packet transmission.
- *Packet drop ratio:*The ratio of the number of delivered data packet to the destination. The greater value of packet drop ratio means the better performance of the protocol.

6. Result and Conclusion

Vehicular Ad hoc Network is a special kind of mobile ad-hoc-network to provide communication among nearby vehicles and between nearby fixed equipment. In this research work, we worked on black hole attack which is the most common attack. We have analyzed the behaviour of the black hole attack. In this paper we have analyzed the blackhole attack using ns2 with different nodes 10,20,30,40.

1. Packet Drop Ratio Analysis

We calculated the packet drop for every 200 sec by calculating the difference of sent packet and receive packets. The following results have been found.

$$\textbf{Packet Drop Ratio} = \frac{\sum(\textbf{Sent Packet} - \textbf{Received Packet})}{\textbf{Sent Packet}}$$

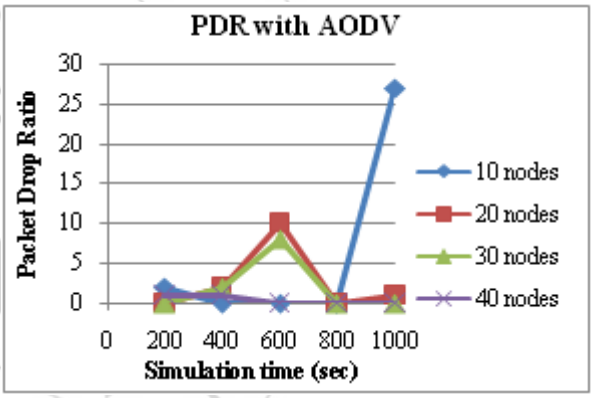

Figure 2: Packet drop ratio with AODV

From the Fig (2) and Fig(3), it is clearly shown that Packet Drop Ratio with Black Hole attack (shown in fig 3) is increased by 5% to 10% with respect to the normal AODV (shown in fig 2).

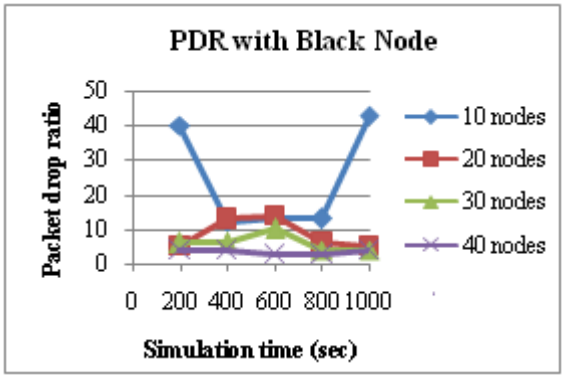

Figure 3: Packet drop ratio with Black node

2. Throughput Analysis

We analyzed the throughput for every 200 sec. Following graphs have been found after the simulation.

Licensed Under Creative Commons Attribution CC BY

$$Avg\ Throughput = \frac{Sum\ of\ bytes\ sent\ through\ the\ data\ packets}{time}$$

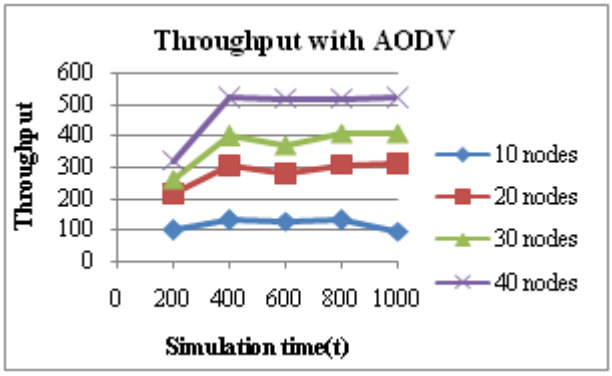

Figure 4: Throughput with AODV

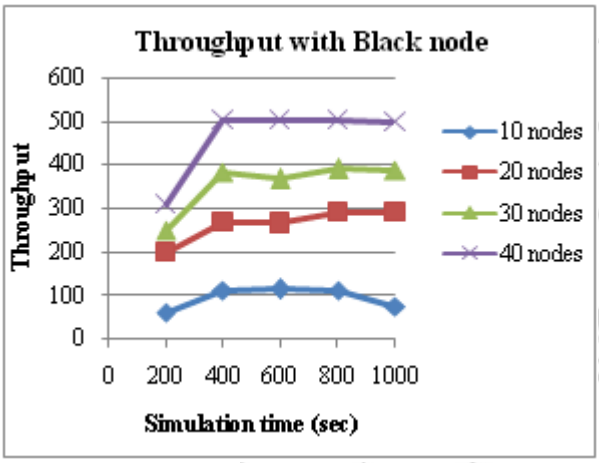

Figure 5: Throughput with Black node

Throughput has been reduced significantly as it is shown in the Fig(4) and Fig(5). It is clear from these graph that throughput has been reduced up to 60-70 kbps due to Black hole attack(shown in fig 5) with respect to the normal AODV(shown in fig 4).

3. End-to end delay

End-to-end delay is, time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in the data packet transmission. Only the data packet that successfully delivered to destination is counted.

$$end-to-end\ delay = \frac{\sum(Arrival\ time\ of\ packet - sending\ time\ of\ the\ packet)}{\sum No.\ of\ connections}$$

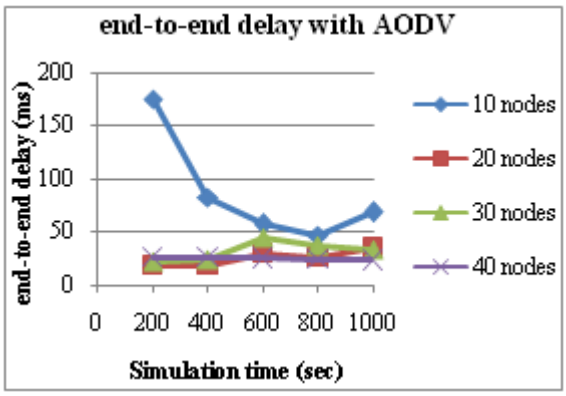

Figure 6: End-to-end delay with AODV

From fig(6) and fig(7). We have seen that the end-to-end delay with Black hole attack (shown in fig 7) is increased 10% to 15% with respect to the normal AODV(shown in fig 6).

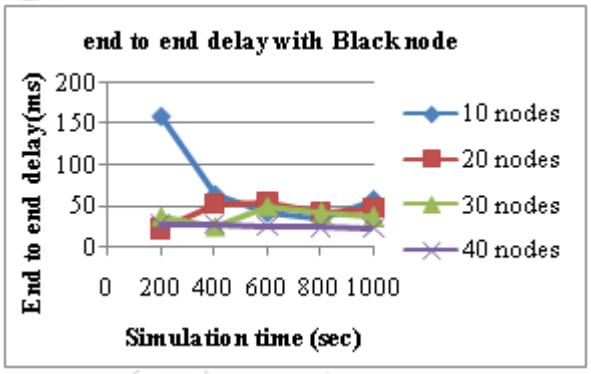

Figure 7: End-to-end delay with Black Node.

From the above graphs we see that when we increase the no. of nodes then the result increased significantly. We also see that the performance of packet drop ratio and end-to end delay in black hole attack is incresedupto 10%-15% respectively with normal AODV.

7. Conclusion

Vehicular Ad-hoc network(VANETs) are a subcategory of Mobile ad-hoc Network which are recently being discussed in great extent. The main intention with VANET"s is to enhance vehicles, passengers, safety and comfort by distributing traffic and other conditions among nearby vehicles.

In this research work, we worked with Black hole attack. We analyzed the behavior of the Black hole attack. In this paper we have analyzed the Black hole attack using ns2 with diff no. of nodes 10,20,30,40with ManhattanGrid scenario. We see that as we increase the no. of nodes then the speed of the vehicles movements increased as shown in the above graphs. We also see that the performance of the black hole attack in packet drop ratio and end-to-end increased but in the throughput is reduced significantly.

8. Future Work

This research work has been carried out for the improvements towards the security of the VANET. This

Licensed Under Creative Commons Attribution CC BY

research work focused only on single attack. In future we would like to perform following tasks regarding Black hole Attack:
Co-operative black hole can be implemented and evaluated.

References

[1] Vimal Bibhu, Kumar Roshan,"*Performance analysis of Black hole Attack in VANET*". International Journal Computer Network and Information security, 2012,11 pp-47-54.
[2] Murthy, C.S.R.Manoj, B.S.:"*Ad- Hoc Wireless Network Architecture and Protocols*". PEARSON.ISBN 81-317-0688-5,(2011).
[3] Sonia and Padmavati,"*Performace analysis of Black hole Attack on VANET'S Reactive Routing Protocols*", International Journal of Computer Applications(0975-8887) Vol. 73-No.9, July 2013.
[4] Network Simulator Official Site for Package Distribution, web reference, *http://www.isi.edu/nsnam.*
[5] Arti Sharma, Satendra Jain, "*A behavioural study of AODV with and without Black hole attack in MANET*". IJMER international Journal of Modern Engineering Research(IJMER), vol. 1 Issue 2. Pp. 391-395.
[6] Sheenu Sharma, Roopam Gupta, "*Simulation Study of Black hole attack in Mobile Ad-hoc Networks*", Journal of Engineering Science and Technology, vol. 4, no.2, 2009. Pp.243-250.
[7] P.Manickam et al., "*Performance comparision of Routing protocols in Mobile ad-hoc Network*". International Journal of wireless and mobile networking(IJWMN). Vol. 3, no. 1, Feb. 2011, pp.98-106.

Licensed Under Creative Commons Attribution CC BY