International Journal on Emerging Technologies (Special Issue NCETST-2017) **8**(1): 516-521(2017)
(Published by Research Trend, Website: www.researchtrend.net*)*

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Performance Analysis of AODV routing protocol under Black Hole Attack in Vehicular Ad-hoc Network (VANET)

Rahul Palaria[1], Amit Joshi[2] and Priyanka Agarwal[3]
[1]Assistant Professor, Amrapali Institute, Haldwani, (U.K.), India
[2]M. Tech. Scholar, Graphic Era Hill University, (U.K.), India
[3]M. Tech. Scholar, GBPUAT,

ABSTRACT: Vehicular Ad-hoc network (VANET) is a self organized & an infrastructure less network. Now a day's VANET becomes a most challenging research area as it has several issues related to its routing protocols, quality of service, security & so on. Vehicular communication is critically unsafe to several kinds of active & passive routing attacks. This paper mainly focuses on Black Hole attack & its effects on Ad-hoc On-Demand Distance Vector (AODV) routing protocol in VANET. Simulation is carried out by using MOVE & NS-2 simulator.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks]: General– Security and protection.
General Terms: Performance, Security.

Keywords: Vehicular Ad-hoc Network (VANET), Black Hole, PDR, Throughput, NRL.

I. INTRODUCTION

Now a day's Vehicular Ad-hoc Network (VANET) becomes a most challenging & promising research area as it has several issues related to its routing protocols, quality of service, security & so on. In VANET, each vehicle or node is equipped with an Application Unit (AU), an On-board Unit (OBU), a Tamper Proof Device (TPD) and a special hardware called Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. All these components are responsible for providing both safety & non safety applications in VANET. Roadside Units (RSUs) also play an important role in vehicular communication by performing a variety of special applications and by transmitting, receiving or forwarding data within the transmission range. VANET is a self organized & infrastructure less networks, which is an evolved structure of Mobile Ad-hoc Network in which every node (vehicle) plays an important role and acts as router to exchange the traffic information with each other within the network coverage area or transmission range. An efficient routing in VANET is a challenging task because of its highly dynamic behavior & frequent link disruption topology, therefore several routing protocols have been proposed in it so that they can easily provide an optimal route from a source node to the targeted destination node. These routing protocols are classified as on-demand (reactive), table driven (proactive) & hybrid routing protocols [1, 2].

Currently, drivers can easily exchange their traffic information and directions with one another by using Vehicular Ad-hoc Network, which provides Intelligent Transportation System (ITS) services such as road safety, efficient driving & infotainment to each & every end user.

In VANET, any node can easily connect and disconnect the network at any instant without informing other nodes in the vicinity. Due this reason, security plays an important role in the deployment of VANET so that all the transmitted information should not be manipulated or dropped by any intruder. In it, Vehicular communication is critically unsafe to several kinds of active and passive attacks such as Denial of Service (DoS), Wormhole, Black Hole, Sybil attack, etc…. [3, 4]

The Black Hole attack is one of the serious types of routing attack which degrades the network performance either by dropping or misusing the intercepted packets without forwarding them [4]. In this paper, we analyze the impact of the Black Hole attack on the AODV routing protocol in VANET.

The remainder of the paper is organized as follows: Section 2 provides an overview of the AODV routing protocol. In section 3, we present a brief analysis of the Black Hole attack. Section 4 presents the simulation

environment including its parameters and performance metrics. In section 5, we analyze the obtained results and the conclusion. Future work is depicted in section 6.

II. OVERVIEW OF AODV

For ad hoc networks, AODV is always considered as one of the most significant routing protocols as it does not maintain the information of the network topology in the routing table at all the time and after that a secure and best suitable path is established only when it is highly required by a source node for sending its data packets to the desired destinations. It is an on-demand (reactive) routing protocol. AODV routing protocol has the ability of both unicast and multicast routing. It mainly consists of four control messages in it: *HELLO, RREQ, RREP, and RERR* [5].

Every node transmits a ***HELLO*** message to all of its neighbor nodes to know about their movement information.

A ***Route Request (RREQ)*** packet is broadcasted from a source node to all of its neighbors if there is no route available for the targeted destination node. The *RREQ* packet structure is as follows [5]:

Source Add.	Source Seq. Num.	Broadcast Id	Dest. Add.	Dest. Seq. Num.	Hop Count

A ***Route Reply (RREP)*** message is received by the source node unicasted by any node in one of the following conditions: if the intermediate node is the targeted destination node or if it is having an optimal route to the targeted destination node in its routing table. The *RREP* packet structure is as follows [5]:

Source Address	Destination Address	Destination Sequence Number	Hop Count	Expiration Time

A node broadcasts a ***Route Error (RERR)*** packet when a link with its neighboring node is broken. The *RERR* packet structure is as follows [6]:

Unreachable Destination IP Address	Unreachable Destination Sequence Number

AODV mainly consists of two processes in it: *Route Discovery process & Route Maintenance process* [5].

The process of Route Discovery is initiated whenever a source node needs to send out all the data packets to a required destination node. In this process, a RREQ packet is broadcasted by a source node to all of its neighboring nodes. After receiving the RREQ packet, an intermediate node checks its routing table and returns a RREP packet to the source node in one of the following cases; if it finds an optimal route to the destination in its routing table or if it is the targeted destination node. Otherwise, the intermediate node rebroadcasts the RREQ packet to its neighbor nodes to get a route from the source node to the destination node as shown in figures 1, 2, & 3.

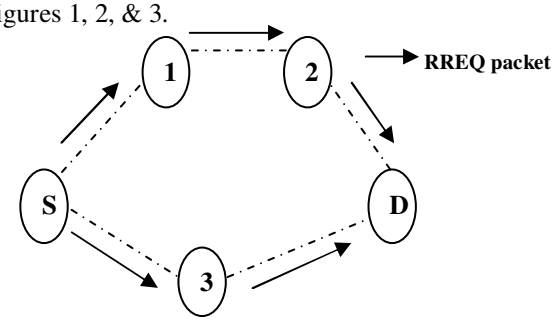

Fig. 1. Route Discovery Process with RREQ packets.

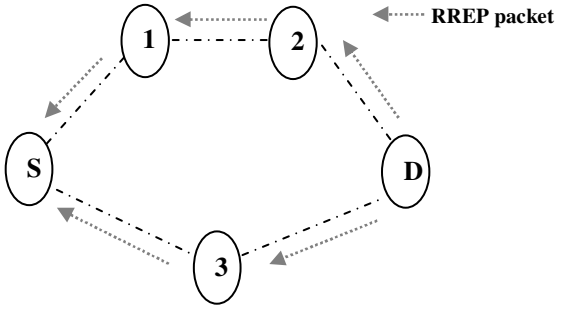

Fig. 2. Route Discovery Process with RREP packets.

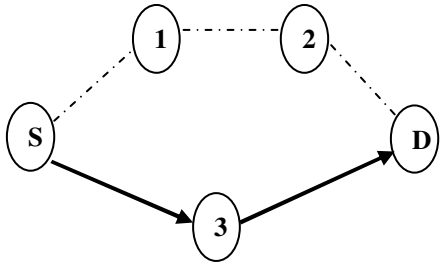

Fig. 2. Route Establishment.

The Route Maintenance process is initiated when a node is unreachable or a link is broken. Active nodes broadcast a HELLO message periodically to get the information about nodes movements. In Route Maintenance process, source node will again initialize a novel or a fresh route discovery process and flood the entire network with RREQ packets to rediscover the path to the destination node as shown in figure 4

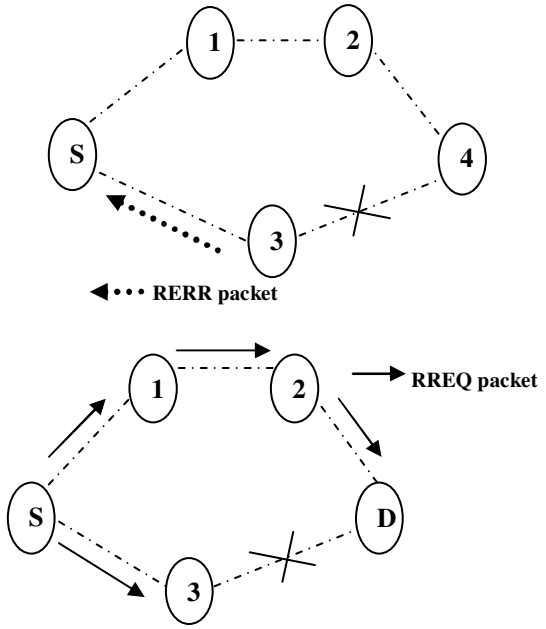

Fig. 3. Route Maintenance Process.

The most significant advantages of the AODV routing protocol are that it offers low overhead & uses sequence numbers to guarantee the novelty of routes.

III. ANALYSIS OF BLACK HOLE ATTACK

The Black Hole attack is one of the serious types of active routing attack in which a malicious node (vehicle) pretends to have an optimum route to the destination, sends fake routing information and indicates that data packets should route through this malicious node [4].

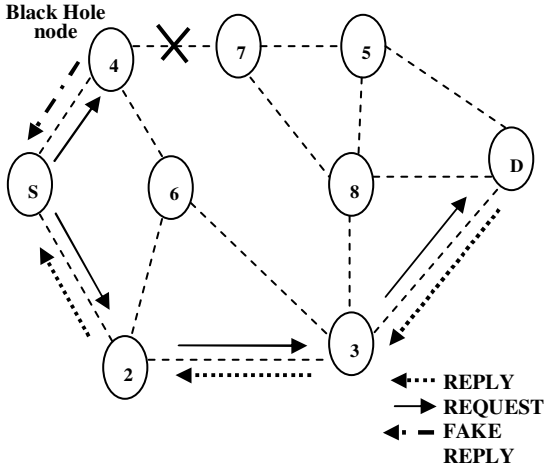

Fig. 4. Black Hole Attack on AODV.

For example, in AODV routing protocol, a malicious node transmits a fake RREP message to the source node. This fake RREP message contains a false destination sequence number which is either greater than or equal to the sequence number held in the RREQ packet. This malicious (Black Hole) node claims that it has a secure and best suitable path to the destination node and indicates that data packets should route through this malicious node; therefore all data traffic will be routed through this malicious node as shown in figure 5 [7].

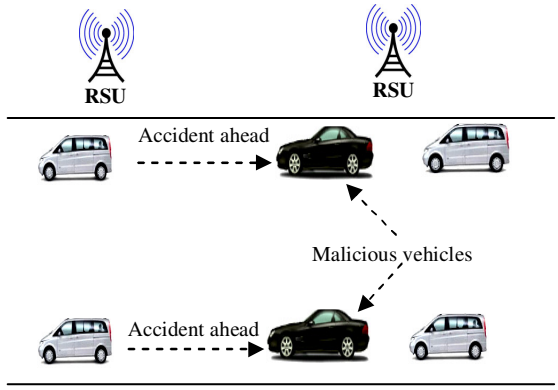

Fig. 5. Black Hole Attack in VANET.

Figure 6 illustrates a Black Hole attack scenario where attack is formed by a number of malicious vehicles & they refuse to broadcast the received messages from the legitimate vehicles to the other legitimate vehicles behind them.

The consequence of the Black Hole attack is that the malicious vehicle can either drop or misuse the intercepted data packets without forwarding them and as a result network performance degrades.

IV. SIMULATION ENVIRONMENT

We have used MOVE (MObility model generator for VEhicular network) tool to generate a realistic mobility model for our VANET simulation. It is based on an open source micro-traffic simulator called Simulation of Urban Mobility (SUMO). MOVE generates a mobility trace file so that it can be later on used by the NS-2.35 simulation tool to provide a realistic model for vehicle movements. In our work, NS 2.35 has been used for the simulation of original AODV and Black Hole AODV. NS-2.35 is an open-source simulation tool which works on Unix-like O.S. It is a discrete event simulator, which is essentially utilized in various networking related researches. It also provides support to simulate various types of protocols like TCP, UDP, FTP, AODV etc…

A. Simulation Parameters

Table 1 illustrates the number of simulation parameters which are used to conduct the simulation of original AODV and Black Hole AODV.

Table 1. Simulation Parameters.

S.No.	PARAMETERS	VALUES
1.	Simulator	NS-2 (Version 2.35)
2.	Routing Protocol	AODV
3.	Channel Type	Channel/WirelessChannel
4.	Simulation Time	100 sec
5.	Network Interface Type	Phy/WirelessPhyExt
6.	Radio Propagation Model	Propagation/TwoRayGround
7.	MAC Type	Mac/802_11p
8.	Interface Queue Type	Queue/DropTail/PriQueue
9.	Antenna	Antenna/OmniAntenna
10.	Traffic Type	CBR (Constant Bit Rate)
11.	Maximum Packet	50
12.	Area (M*M)	910*500
13.	Number of nodes (vehicles)	20
14.	Number of malicious node (vehicle)	1

B. Performance Analysis

We examined the performance of AODV routing protocol by analytical study of measures of different types of performance metrics in VANET. These performance metrics are as follows [8-10]:

Packet Delivery Ratio (PDR): In the theoretical parlance, PDR is considered as the ratio of the total number of received packets by the destination node to the total number of transmitted packets by the source node. The protocol provides better performance if it has the greater value of PDR.

$$PDR = \frac{\sum Number\ of\ received\ data\ packets}{\sum Number\ of\ sent\ data\ packets}$$

Throughput: In the theoretical parlance, Throughput is measured as the total number of packets transmitted by a source to the respective destination node at per unit of time. It is measured as the received throughput in bit per sec (b/s) at the traffic destination.

Normalized Routing Load (NRL): In the theoretical parlance, NRL is considered as the total number of routing packets transmitted as an overhead to resolve the routing for a unit of data packets received at the destination node.

$$NRL = \frac{Total\ number\ of\ routing\ packets\ sent}{Total\ number\ of\ received\ data\ packets}$$

Number of dropped packets: It is considered as the measure of the number of dropped packets from the nodes. The protocol provides better performance if it has the lowest value of number of dropped data packets. Number of dropped data packets = Number of sent data packets - Number of received data packets

V. RESULT ANALYSIS

In this, we analyze the obtained results of AODV and Black Hole AODV.

A. Packet Delivery Ratio (PDR)

Figure 7 illustrates that the values of PDR increases linearly for original AODV as compared to the PDR values for Black Hole AODV which are low & decreases sharply when we vary node mobility from 30m/s to 40 m/s.

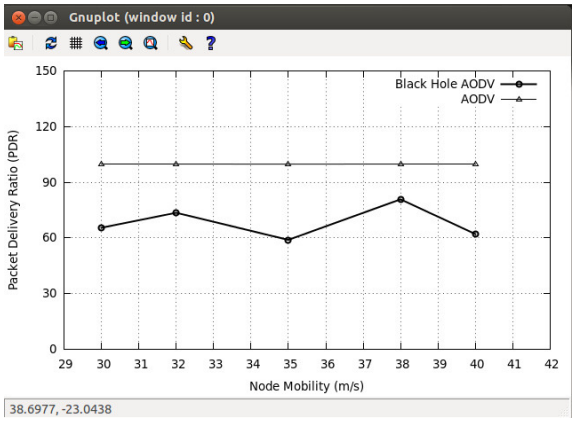

Fig. 7. PDR vs. Node Mobility.

B. Throughput

Figure 8 illustrates that the Throughput values for original AODV increases linearly as compared to the Throughput values for Black Hole AODV which are low & decreases sharply when we vary node mobility from 30m/s to 40 m/s.

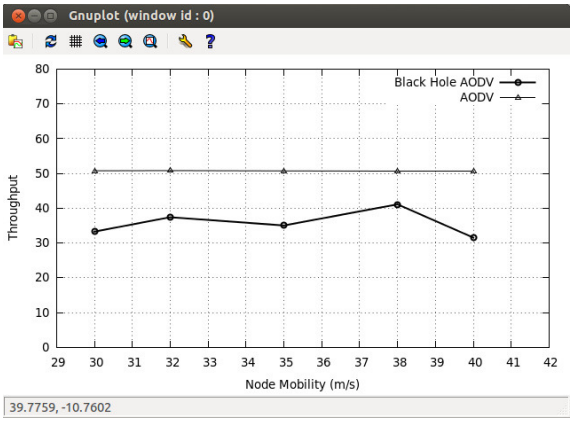

Fig. 6. Throughput vs. Node Mobility.

C. Normalized Routing Load (NRL)

Figure 9 illustrates that the NRL values for original AODV decreases sharply as compared to the NRL values for Black Hole AODV which are high when we vary node mobility from 30m/s to 40 m/s.

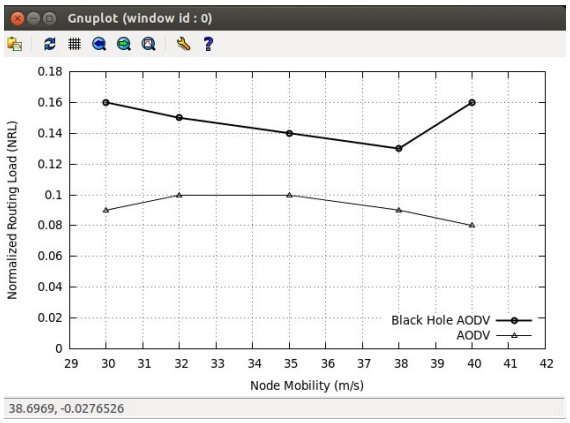

Fig. 9. NRL vs. Node Mobility.

D. Number of dropped packets

Figure 10 illustrates that the Number of dropped data packets for original AODV is low (2-4 packets) when we vary node mobility from 30m/s to 40m/s.

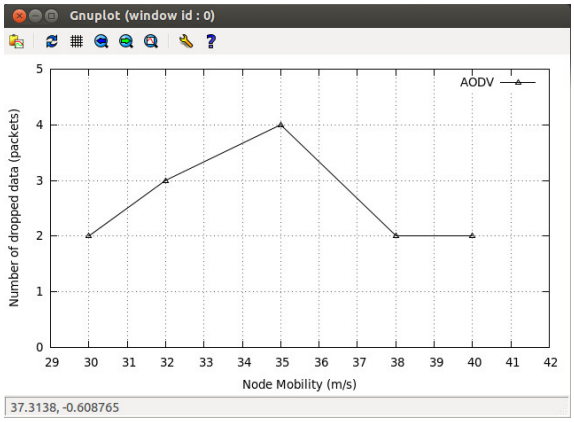

Fig. 10. Number of dropped packets vs. Node Mobility.

Figure 11 illustrates that the Number of dropped data packets for Black Hole AODV is high (200-500 packets) when we vary node mobility from 30m/s to 40m/s.

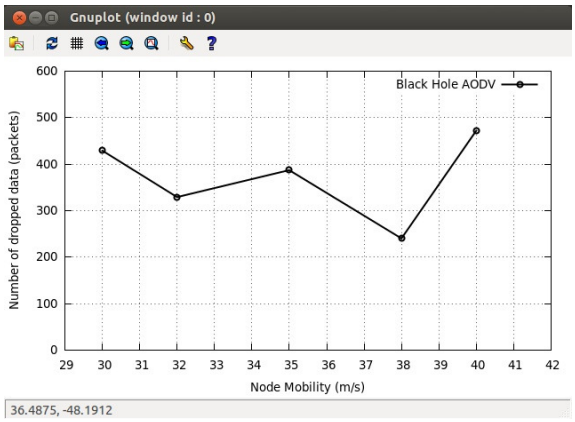

Fig. 11. Number of dropped packets vs. Node Mobility.

Table 2. Comparison of performance metrics of AODV with & without Black Hole Attack.

S.No.	Node Mobility (m/s)	Simulation Results with Black Hole Attack				Simulation Results without Black Hole Attack			
		PDR	Throughput	NRL	Number of Dropped Packets	PDR	Throughput	NRL	Number of Dropped Packets
1.	30	65.43	33.28	0.16	429	99.84	50.79	0.09	2
2.	32	73.5	37.42	0.15	329	99.84	50.83	0.10	3
3.	35	58.89	35.05	0.14	387	99.76	50.75	0.10	4
4.	38	80.74	41.11	0.13	240	99.84	50.79	0.09	2
5.	40	62.04	31.56	0.16	472	99.84	50.79	0.08	2

PDR: Packet Delivery Ratio, NRL: Normalized Routing Load

VI. CONCLUSION & FUTURE WORK

There are various active and passive routing attacks which affect the performance of vehicular communication. In Vehicular Ad-hoc Network (VANET), the Black Hole attack is considered as one of the severe types of active routing attack. In our work, we have analyzed the effect of the Black Hole attack on the AODV routing protocol in VANET. To study the effect of the Black Hole attack on AODV, we choose following performance metrics; PDR, Throughput, NRL and Number of dropped packets & analyze them carefully. We examined that the functioning of the AODV routing protocol is degraded heavily under the influence of Black Hole attack in VANET.

In our future work, we will propose an efficient & effective solution or technique which can easily detect & mitigate the Black Hole attack & can enhance the performance of the AODV routing protocol in VANET to provide a secure vehicular communication in it.

REFERENCES

[1]. Lin, X., et al., Security in vehicular ad hoc networks. *Communications Magazine, IEEE, 2008.* **46**(4): p. 88-95.

[2] Dua, A., N. Kumar, and S. Bawa, A systematicre view on routing protocols for Vehicular Ad Hoc Networks. Elsevier Inc., 2014(Vehicular Communications1(2014)).

[3] Zeadally, S., et al., Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems, 2012. **50**(4): p. 217-241.

[4] Al-kahtani, M.S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on. 2012.

[5] Perkins, C.E. and E.M. Royer. Ad-hoc on-demand distance vector routing. in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on. 1999.

[6] Gandhewar, N. and R. Patel. Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network. in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. 2012: IEEE.

[7] Kannhavong, B., et al., A survey of routing attacks in mobile ad hoc networks. Wireless communications, IEEE, 2007. **14**(5): p. 85-91.

[8] Simaremare, H. and R.F. Sari, Performace Evaluation of AODV variants on DDoS, Blackhole and Malicious Attacks. IJCSNS, 2011. **11**(6): p. 277-287.

[9] Shrivastava, L., S.S. Bhadauria, and G.S. Tomar. Performance Evaluation of Routing Protocols in MANET with Different Traffic Loads. in Communication Systems and Network Technologies (CSNT), 2011 International Conference on. 2011: IEEE.

[10] Shah, S., et al., Performance evaluation of ad hoc routing protocols using NS2 simulation. Mobile and Pervasive Computing (CoMPCâ€“2008), 2008: p. 167-171.