RESEARCH ARTICLE OPEN ACCESS

Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack

T.Sairam Vamsi1, E.R. Praveen Kumar2, T.Sruthi3
1, 2,3Assistant Professor, Shri Vishnu Engineering College for Women, Bhimavaram, A.P
Corresponding Author: T.Sairam Vamsi

ABSTRACT: The Mobile Ad hoc Network (MANET) is a collection of portable devices establishing intermediate network without any access points. These MANETs plays a vital role in present wireless communication world. But these MANETs are highly vulnerable to attacks due to their characteristics such as the lack of infrastructure and wireless communication. This project deals with Ad Hoc On-demand Distance vector (AODV) routing protocol which is intended for use by mobile nodes in an ad hoc network. With the help of AODV protocol, the routing behavior can be analyzed by considering different parameters like throughput, delay, load and number of packets dropped using network simulator (NS2). There are different attacks, which damages the network like warm-hole, black-hole, jamming attacks etc. due to these attacks the performance of network is effected greatly. Out of all, black hole attack is one kind of routing distributing attacks and can bring great damage to the network. Here this project uses the AODV's sequence number for identifying the Black-hole node in the network without using any extra packet formats. This project analyses throughput, delay, and load, number of packets dropped with and without attack in the MANET using NS2 simulator.
Key words: AODV, proactive, reactive, hybrid, black hole, throughput, load, delay.

Date Of Submission: 09-05-2019 Date Of Acceptance: 24-05-2019

I. INTRODUCTION

WSN refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSN measure environmental conditions like temperature, sound, pollution, etc..

1.1 Objective:

The main objective of this paper is to analyze the AODV protocol with different parameters like throughput, delay, number of packets dropped at the destination node in Mobile Ad Hoc Network (MANET) with and without black hole attack using NS2 Simulator.

1.2 Scope of the Paper:

The two categories of routing protocols called as Reactive, proactive, and the derived one from reactive and proactive protocols are referred to as hybrid routing protocol. The hybrid protocol is a combination of both reactive and proactive routing protocols. In this thesis, a reactive routing protocol which is AODV is considered.

In this research work the behavior of above mentioned AODV routing protocol will be evaluated when implemented in the network and look that how this protocol affect the network performance, and how they behave in these networks. The algorithm design and analysis of this routing protocol will not be the focus however a detailed explanation of this routing protocol and its effects on the network will be discussed.

II. PERFORMANCE OF PARAMETERS

There are different kinds of parameters for the performance evaluation of the routing protocols. These have different behaviors of the overall network performance.

PDR: The packet end-to-end delay is the time of generation of a packet by the source up to the destination reception. So this is the time that a packet takes to go across the network. This time is expressed in sec. Hence all the delays in the network are called packet end-to-end delay, like buffer queues and transmission time.

Number of packets dropped: Packet drop occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet drop is either caused by errors in data transmission, typically across wireless network or network congestion. Packet drop is measured as a percentage of packets lost with respect to packets sent.

Throughput: Throughput is defined as, the ratio of the total data reaches a receiver from the sender. The time it takes by the receiver to receive the last message is called as throughput. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).

III. ATTACKS

The attacks can come from both inside the network and from the outside. A mobile ad hoc network (MANET) is a self-configuring network of mobile nodes, so it is vulnerable with so many attacks while data is travelling in network.

Attacks are classified into two categories DATA traffic attacks and CONTROL traffic attacks. This classification is based on their common characteristics and attack goals. For example: Black-Hole attack drops packets every time, while Gray-Hole attack also drops packets but its action is based on two conditions: time or sender node. But from network point of view, both attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack when it starts dropping packets. So they can be categorized under a single category. There are four types of attacks

- Black hole attack
- Gray hole attack
- Warm hole attack
- Jellyfish attack

3.1 Black hole attack: MANET is susceptible to many security attacks. Black Hole Attack is one of these attacks. It is a simple but certainly effective Denial of Service attack in which a malicious node, through its routing protocol, advertises itself for having the shortest path to the destination node or to the node whose packets it wants to intercept. It pretends to have enough of fresh routes for a certain destination. The source node assumes it to be true and the data packets are forwarded to a node which actually does not exist, causing the data packets to be lost. When a source node wants to initiate the communication, it broadcasts a RREQ message for route discovery. As soon as the malicious node receives this RREQ packet, it immediately responds with a false RREP message to the respective node advertising itself as the destination or having the shortest path for that destination.

IV. SIMULATION OUTPUTS

This paper will analyze and discuss the results of simulations that are done. Simulation begins with the analysis of AODV routing protocol by three parameters such as delay, packets dropped, and throughput with and without attack. The results obtained in the form of graphs, all the graphs are displayed as average.

4.1 SIMULATION STEPS:

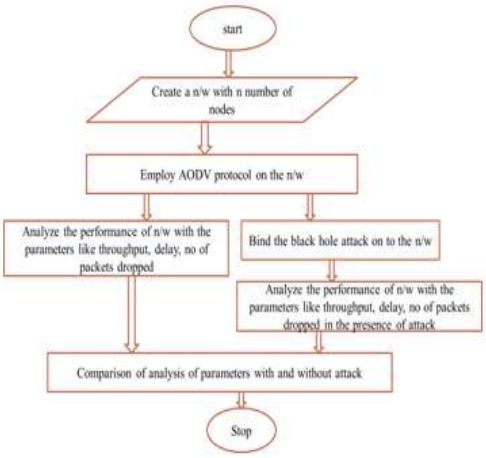

Fig 4.1: Simulation steps

4.2 SIMULATION OF SCENARIO:

for determining the parameters. Parameters like throughput delay and packets drooped are determined by using the trace file format and Fig 4.4 and fig 4.5 shows the nam files with and without black hole attack which shows how the transmission of data packets done between the nodes. The network size is of 1600 x 2400 meters. The CBR was selected as traffic High Load. The protocol such as AODV is tested against three parameters i.e. delay, number of packets dropped and throughput with and without attack.

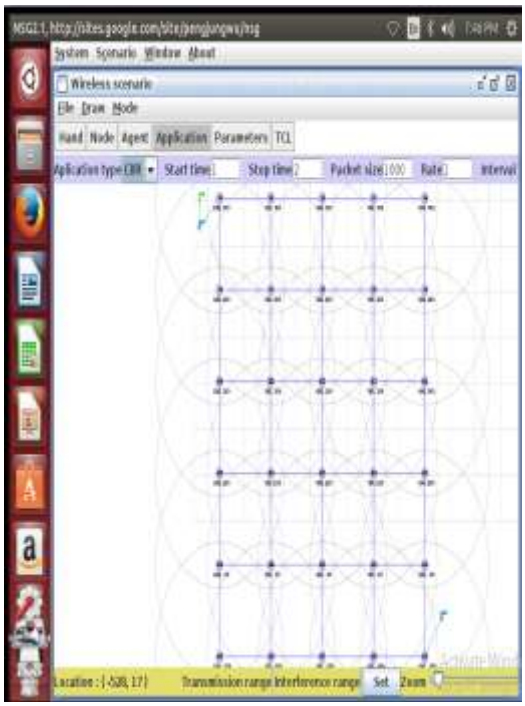

Fig 4.2: Scenario for 30 nodes

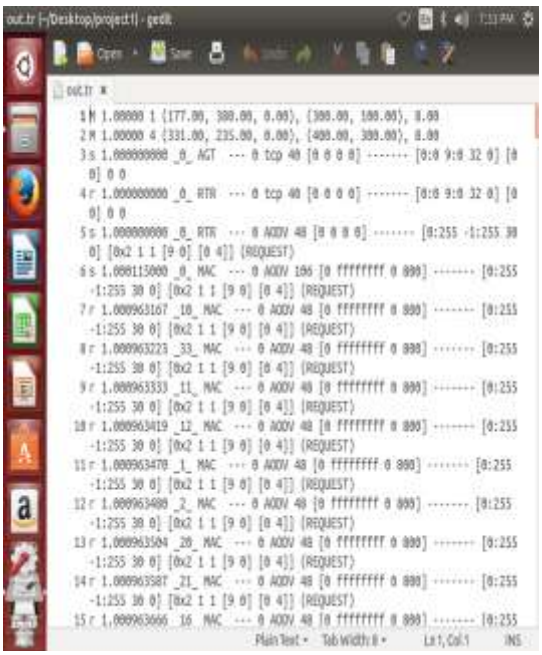

Fig 4.3: Trace file

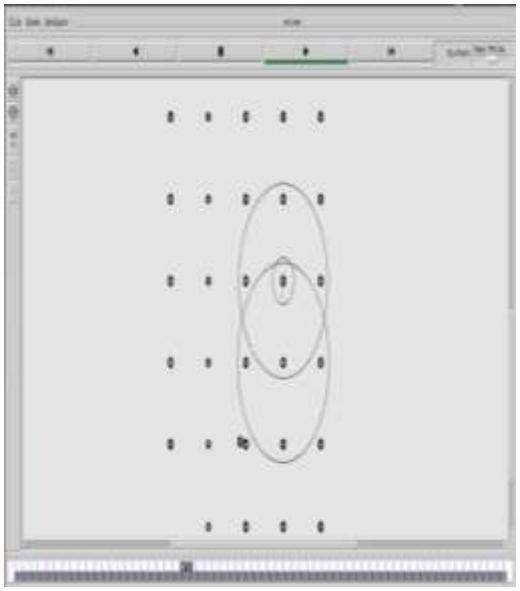

Fig 4.4: nam file without black hole attack

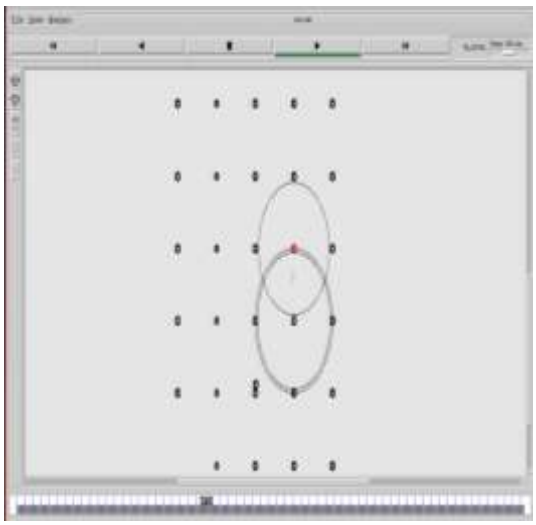

Fig 4.5: nam file with black hole attack

4.3 AODV PERFORMANCE:

The scenario is simulated and it gives the required results shown in the below figures. The Ad hoc On Demand Distance Vector protocol was checked by three parameters such as delay, packets dropped and throughput. The graphs are shown in the time average form.

End-to-end delay:

The below graph is plotted by taking all the values of end to end delay of all the scenarios consisting different number of nodes with and without the presence of black hole attack for one and two mobile nodes differently. In the below Fig 4.6 and Fig 4.7, X-axis represents no of nodes in the network and Y-axis represents end to end delay.

For 1 mobile node

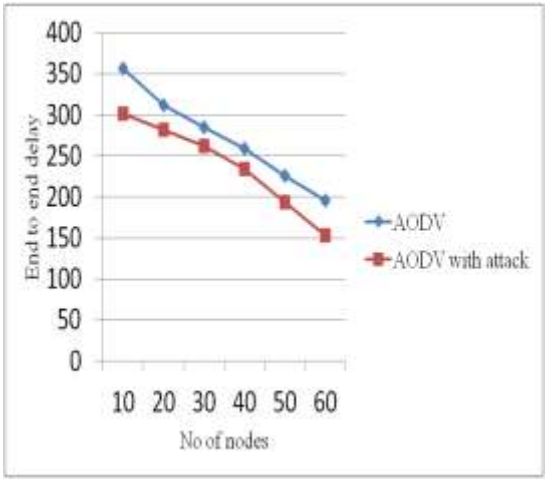

Fig 4.6: No of nodes Vs. End to end delay (one mobile node)

For 2 mobile nodes:

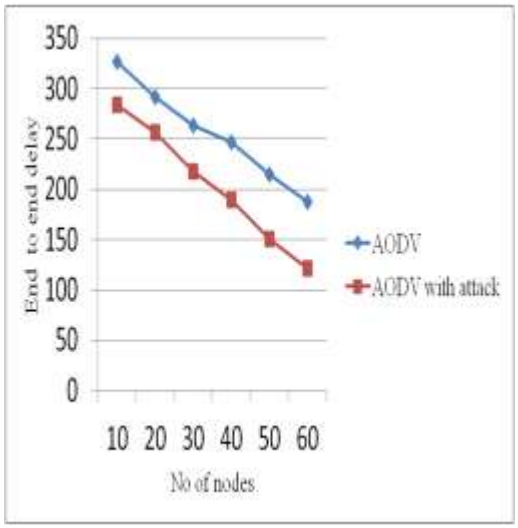

Fig 4.7: No of nodes vs. end to end delay (two mobile nodes)

Packets dropped:

The below graph is plotted by taking all the values of number packets dropped in all the scenarios when compared to the generated packets with and without the presence of black hole attack for one and two mobile nodes differently in the network. In the below Fig 4.8 and Fig 4.9, X-axis represents no of nodes in the network and Y-axis represents number of packets dropped.

For one mobile node:

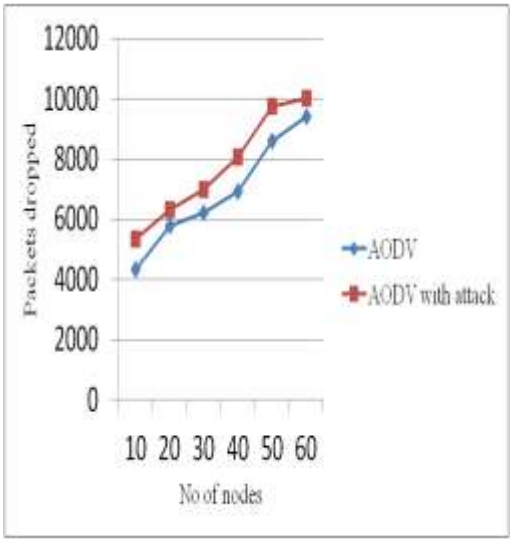

Fig 4.8: No of nodes vs. packets dropped (one mobile node)

For two mobile nodes:

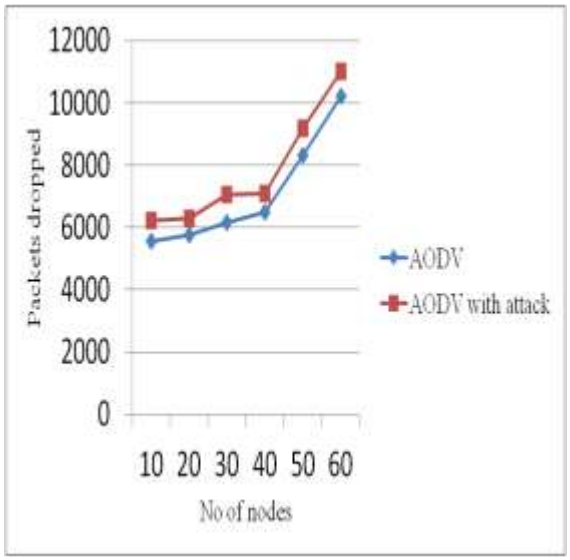

Fig 4.9: No of nodes vs. packets dropped (two mobile nodes)

Throughput:

The below graph is plotted by taking all the values of throughput of all the scenarios consisting different number of nodes with and without the presence of black hole attack for one and two mobile nodes differently. In the Fig 4.10 and Fig 4.11, X-axis represents no of nodes in the network and Y-axis represents throughput.

For one mobile node:

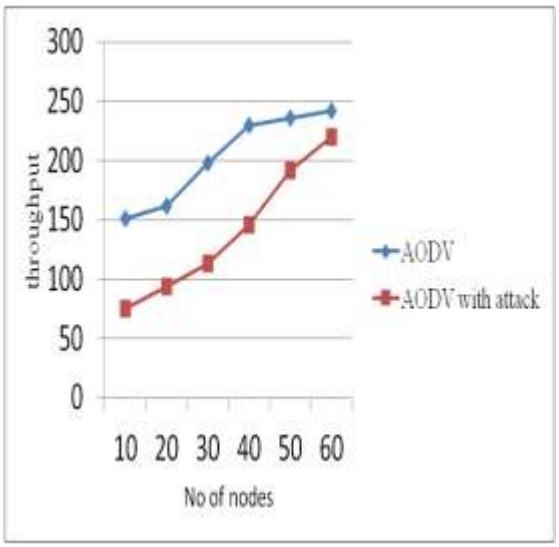

Fig 4.10: No of nodes vs. Throughput (one mobile node)

For two mobile nodes:

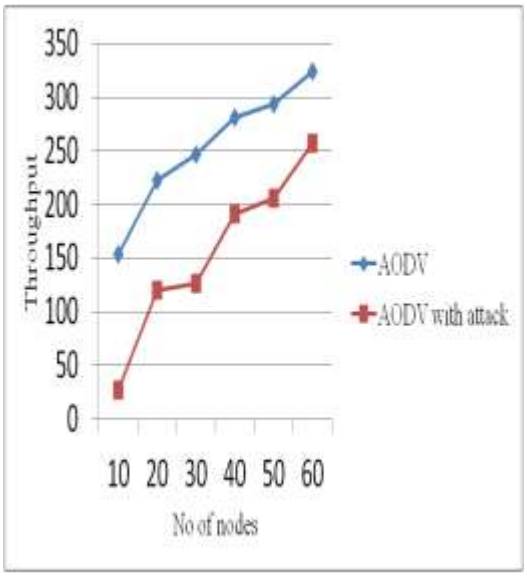

Fig 4.11: No of nodes vs. throughput (two mobile nodes)

4.4 COMPARATIVE ANALYSIS:

The below Table 4.1 gives comparative analysis of end to end delay caused in the network with and without the presence of black hole attack for 2 and 3 mobile nodes where AODV protocol is used for routing.

Table 4.1: values of end to end delay with and without attack

No of nodes	Delay for 1 mobile node		Delay for 2 mobile nodes	
	Without attack	With attack	Without attack	With attack
10	356.64	301.56	326.45	283.65
20	312.56	281.95	291.62	256.36
30	285.34	261.73	263.94	217.92
40	258.71	234.21	247.19	189.43
50	226.35	193.65	214.95	150.57
60	196.23	153.69	187.23	121.74

The below Table 4.2 gives comparative analysis of number of packets dropped caused in the network with and without the presence of black hole attack for 2 and 3 mobile nodes where AODV protocol is used for routing.

Table 4.2: values of packets dropped with and without attack

No of nodes	Packets dropped for 1 mobile node		Packets dropped for 2 mobile nodes	
	Without attack	With attack	Without attack	With attack
10	4338	5329	5546	6213
20	5766	6308	5763	6308
30	6201	6984	6149	7055
40	6912	8079	6478	7079
50	8599	9745	8317	9199
60	9432	10036	10220	11019

The below Table 4.3 gives comparative analysis of throughput caused in the network with and without the presence of black hole attack for 2 and 3 mobile nodes where AODV protocol is used for routing.

Table 4.3: values of throughput with and without attack

No of nodes	Throughput for 1 mobile node		Throughput for 2 mobile nodes	
	Without attack	With attack	Without attack	With attack
10	151.19	75.69	154.05	76.79
20	161.82	93.57	222.12	120.41
30	198.18	113.48	246.98	125.84
40	230.01	145.98	280.75	191.71
50	235.58	192.15	293.73	205.63
60	241.71	220.45	324.14	256.8

V. CONCLUSIONS

In all the scenarios simulated and studied, it is noticed, with the black hole attack the network parameter degrades. With the increase in network traffic, throughput and PDR increases and packet drop decreases under no attack condition. It is also observed that when the attacker is near the source the impact is severe than it is farther. Similarly as the number of black hole increases, PDR and throughput decreases. In all the simulations the proximity of attacker to the sending node has impact on the average delay and it decreases with black hole attack. This is due of the fact that the black hole sends the RREP with highest destination sequence number without verifying for a route in its routing table. Many researchers have proposed different types of prevention schemes by modifying basic AODV protocol.

REFERENCES

[1]. **T.Sairam Vamsi,** Ramya P**,** Dr.G.R.L.V.N.S Raju "**A Survey on Underground Distributed Wireless Sensor Networks:Design & Research Challenges**" in International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN:2250-3501, Volume-07, Issue-06, pp.05-08.

[2]. Mr.K.Murthyraju,Dr.K.MallikarjunaPrasad, **Mr.T.Sairam vamsi** "**Enhanced Energy Accuracy**

based on clustering ” in International Journal of Engineering Trends and Technology (IJETT) ISSN:2231-5381, Volume-42, Issue-3, pp.146-152.

[3]. Mohebi, Amin and Kamal, Ehsan and Scott, Simon, “Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack,” International Journal of Modern Education \& Computer Science, vol. 5, 2013.

[4]. Gupta, S Balaji and Navneeth, T and Sundar, S and Vidhyapathi, CM, Performance Evaluation of MANET Routing Protocols under Varying Node Mobility,” International Journal of Engineering \& Technology (0975-4024), vol. 5, 2013.

[5]. Singh, S. (2014). Maodv: To identify a secure route selection in manet under blackhole. Master's thesis, ShaheedBhagat Singh State Technical Campus.

[6]. Nor SurayatiMohamadUsop, Azizol Abdullah, Ahmad Faisal AmriAbidin, ‘‘Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment’’, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009

[7]. Xiaogeng Zhao, ‘‘An Adaptive Approach for Optimized Opportunistic Routing Over Delay Tolerant Mobile Ad Hoc Networks’’, Computer Science Department, December 2007

[8]. Julian Hsu, Sameer Bhatia, Ken Tang, RajiveBagrodia, Scalable Network Technologies, Inc., Culver City, CA . Michael J. Acrkhe US ARMY RDECOM CERDEC STCD, ‘‘PERFORMANCE OF MOBILE AD HOC NETWORKING ROUTING ROTOCOLS IN LARGE SCALE SCENARIOS’’, MILCOM 2004 - 2004 IEEE Military Communications Conference.

[9]. Ramya P, **SairamVamsi T**, “Impact Analysis of Blackhole,Flooding and Grayhole Attacks and Security Enhancements in Mobile Ad Hoc”, Attended conference on International conferenceonMicroElectronics,Electromagnetics and Telecommunications(ICMEET 2017) organized by BVRIT, Hyderabad, 9th and 10thSeptember 2017.

[10]. Ramya P, **SairamVamsi T**, “Securing MANETs using SHA3 Keccak Algorithm”, Attended conference on International computing and communication technologies(ICICCT 2019) organized by BVRIT, Hyderabad, 9th and 11th January 2019.

T.Sairam Vamsi" Performance Analysis of Aodv Routing Protocol in Manet under Blackhole Attack" International Journal of Engineering Research and Applications (IJERA), Vol. 09, No.05, 2019, pp. 58-63