International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.1, Issue.2, pp-391-395 ISSN: 2249-6645

A Behavioral Study of AODV with and without Blackhole Attack in MANET

Arti Sharma and Satendra Jain
SATI, Vidisha, India

Abstract- Wireless mobile ad-hoc networks are those networks which has no physical links between the nodes. Due to the mobility of nodes, interference, multipath propagation and path loss there is no fixed topology in this network. Hence some routing protocol is needed to function properly for these networks. Many Routing protocols have been proposed and developed for accomplishing this task. The intent of this paper is to analyze the performance of ad-hoc routing protocol AODV with and without black hole attack in wireless network. This paper concentrates evaluating the performance of routing protocol when black hole attacks involve in wireless network and when black hole attack not involve in wireless network. The performance analysis for above protocol is based on variation in speed of nodes in a network with 50 nodes. All simulation is carried out with QualNet 5.0 simulator.

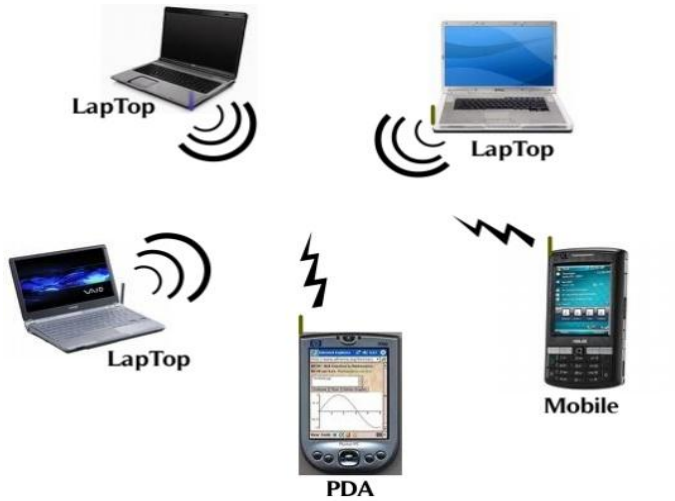
Keywords: *Ad Hoc Networks, routing protocol, Black hole attack, AODV.*

I. INTRODUCTION

Mobile ad hoc networks (MANETs) [1,2] are collections of mobile nodes, which are Dynamically form a temporary network without pre-existing network infrastructure or any centralized administration. These nodes can be arbitrarily located and are free to move randomly at any given time. Every mobile node acts itself as a router. Since there is no centralized administration, so MANET is oftenly called autonomous. MANET implies that the topology may be dynamic - and that routing of traffic through a multi-hop path is necessary if all nodes are to be able to communicate. A key issue in MANETs is the necessity that the routing protocols must be able to respond rapidly to topological changes in the network. At the same time due to the limited bandwidth available through mobile radio interfaces it is imperative that the amount of control traffic generated by the routing protocols is kept at a minimum. Several protocols have been addressed these problems of routing in mobile ad-hoc networks. These protocols were divided into two classes: depending upon the type of requirement and the available resources, when a node acquires a route to a destination.

Proactive protocols [3] are characterized by all nodes maintaining routes to all destinations in the network at all times. Thus using a proactive protocol a node is immediately able to route (or drop) a packet. Examples of proactive protocols include the "FISHEYE". [25], the "Optimized Link State Routing Protocol" (OLSR) [9] and the "Source Tree Adaptive Routing" (STAR) [6]. *Hybrid* protocols [3, 4] are those protocols which have characteristics of both reactive and proactive. Example of hybrid protocol includes "Dynamic MANET On-demand routing protocol" (DYMO) [27].

Reactive protocols [3] are characterized by nodes acquiring and maintaining routes ON-demand. In general, when a route to an unknown destination is required by a node, then the route request is flooded onto the network and replies, containing possible routes to the destination, are returned. Examples of reactive protocols include the "Ad Hoc on Demand Distance Vector Routing Protocol" (AODV) [27] and "Dynamic Source Routing" (DSR) [5].



In this paper, the analysis of routing protocol AODV is presented against black hole attack. The performance of this protocol is analyzed with varying speed of nodes in network. The network contains 50 wireless nodes in which 10 nodes are in black hole attack. These nodes either stop packet forwarding or send wrong and unusual information to other nodes which affects packet drop and lesser throughput.

The organization of this paper is as follows. Section 2 briefly describes the routing protocols AODV. Section 3 briefly describes the affects of black hole attack in network. Section 4 presents experimental configuration. Section 5 focused on results and analysis of the work and Section 6 represents a conclusion of the paper.

II. ROUTING PROTOCOLS

The nature of mobile ad hoc networks makes simulation modeling an invaluable tool for understanding the operation of these networks. In Ad-hoc network multiple routing protocols have been developed during the last years, to find optimized routes from a source to some destination. To establish a data transmission between two nodes, typically multiple hops are required due to the limited transmission range. Mobility of the different nodes makes the situation even more complicated.

The protocols to be used in the Ad Hoc networks should have the following features:

- The protocol should adapt quickly to topology changes.
- The protocol should provide Loop free routing.
- The protocol should provide multiple routes from the source to destination and this will solve the problems of congestion to some extent.
- The protocol should have minimal control message overhead due to exchange of Routing information when topology changes occurs.
- The protocol should allow for quick establishment of routes so that they can be used before they become invalid.

Ad hoc On-Demand Distance Vector (AODV) [27]

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and unicast route determination to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.
The primary objectives of AODV protocol are [27]:

- To broadcast discovery packets only when necessary,
- To distinguishes between local connectivity management (neighborhood detection) and general topology maintenance and
- To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information. AODV decreases the control overhead by minimizing the number of broadcasts using a pure on-demand route acquisition method. AODV uses only symmetric links between neighboring nodes.

III. BLACK HOLE ATTACK

In Blackhole attack all networks traffics are redirected to a specific node which does not exist at all.Because traffics disppear into the special node as the matter disappears into Blackhole in universe .So the specific node is named as a Blackhole.A Blackhole has two properties.First, the node exploits the ad hoc routing protocol,such as AODV , to advertise itself as having a valid route to a destination node, even though the route is spurious,with the intention of intercepting packets. Second, the node consumes the intercepted packets.

IV. EXPERIMENT CONFIGURATION

All the simulation work is performed in QualNet wireless network simulator version 5.0 [3]. Initially number of nodes are 50, simulation time was taken 180 seconds . All the scenarios have been designed with a terrain 1500m x 1500m. Mobility model used is Random Way Point [26] (RWP). In this model a mobile node is initially placed in a random location in the simulation area. For simulation, speed of node is varying from 10mps to 50mps. All the simulation works were carried out using routing protocol AODV with varying speed of node. Network traffic load is provided by constant bit rate (CBR) application. A

CBR traffic source provides a constant stream of packets throughout the whole simulation, thus further stressing the routing task. There are four measurements in our experiments were defined as follows:

1) *Throughput (bits/s):-* Throughput [26] is the measure of the number of packets successfully transmitted to their finaldestination per unit time.

2) *Total Packets received:* - Packet delivery ratio **[27]** is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).

***3) End-to-end delay*:** Average End to End Delay **[27]** signifies the average time taken by packets to reach one end to another end (Source to Destination)**.**

4) Average Jitter Effect: Signifies the Packets from the source will reach the destination with different delays [5]. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

V. SIMULATION RESULTS & ANALYSIS

a. Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets.

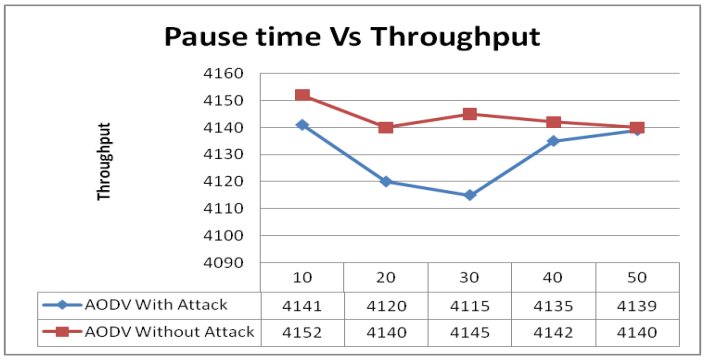


Figure1:- Pause Time Vs Throughput

Figure 1 shows throughput of AODV in presence and without presence of black hole attack with variation of pause time. It is observed that throughput of AODV is rises without presence of attack. It can also be observed that throughput of AODV in both conditions are same at pause time 50s.

b. Average End to End Delay signifies the average time taken by packets to reach one end to another end (Source to Destination).

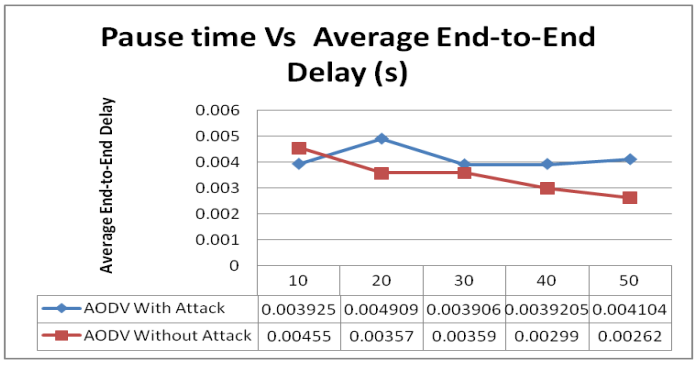


Figure2:- Pause Time Vs Average End-to-End delay

Figure 2 shows end to end delay of AODV in presence and without presence of black hole attack with variation of pause time. It can observe that end to end delay is goes down when AODV works without black hole attack in network. But it end to end delay in presence of black hole at pause time 10 is less then without presence of attack.

c. Total packets received are no. of packets received when sent from source to destination

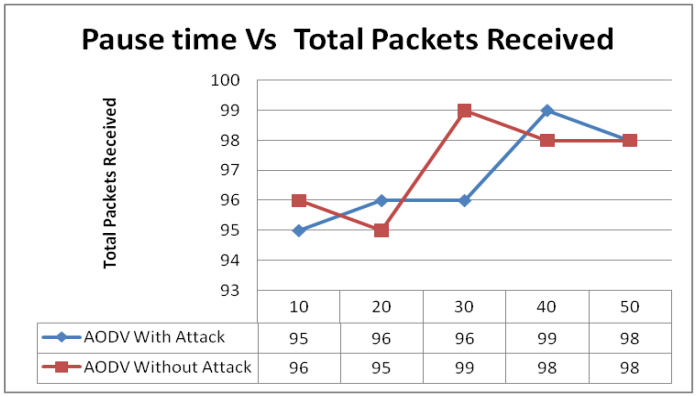


Figure3:- Pause Time Vs Total Packets Received

Figure 3 shows total packet received of AODV in presence and without presence of black hole attack with variation of pause time. It can be observed that performance of AODV without attack performs well. Receiver can receive packet due to better routing technique and route caching. It is also observed that there is fewer packets have received when pause time is 20s. The reason behind it is the signal coverage or mobility of nodes.

d. Average Jitter effect signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

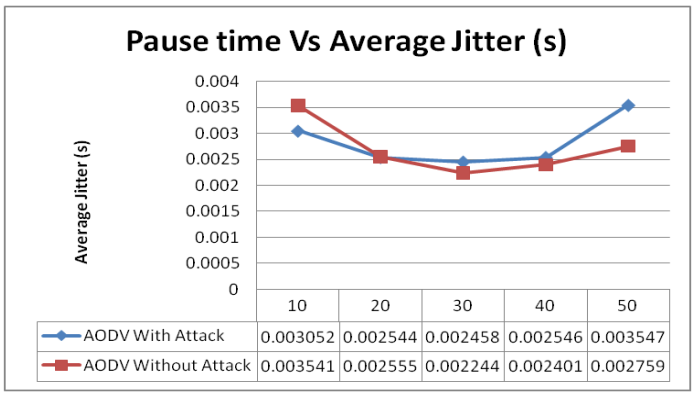


Figure4:- Pause Time Vs Average Jitter

Figure 4 shows average jitter of AODV in presence and without presence of black hole attack with variation of pause time. It is observed that Avg. jitter effect in AODV without attack and AODV with attack changes by increasing or decreasing the pause time. The Jitter effect decreases as the pause time increases. But when it becomes 50s average jitter increases for each protocol.

e. Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets.

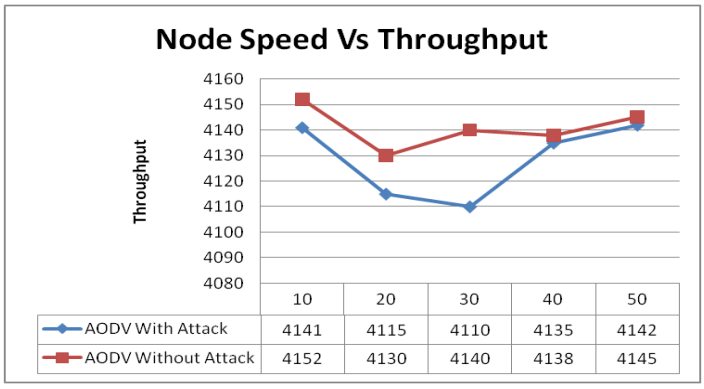


Figure5:- Node Speed Vs Throughput

Figure 5 shows throughput of AODV in presence and without presence of black hole attack with variation of speed of node in network. It can be observed that when node speed is 50m/sec then throughput for AODV without attack is similar to throughput of AODV with attack. It can be observed that throughput of protocol are decreases when nodes in network moving with speed of 20m/sec, and it also varies with different node speeds.

f. Average End to End Delay signifies the average time taken by packets to reach from one end to another end (Source to Destination).

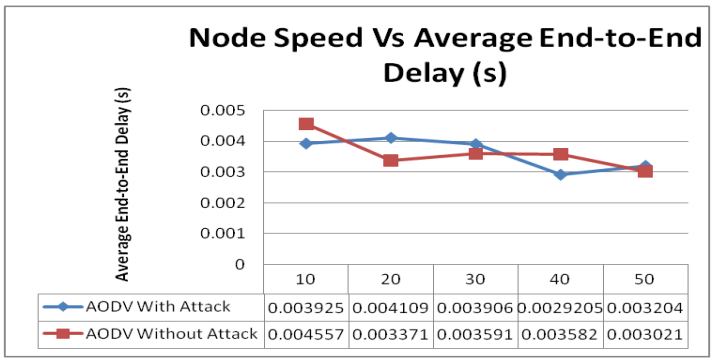


Figure6:- Node Speed Vs Average End-to-End delay

Figure 6 shows average end-to-end delay of AODV in presence and without presence of black hole attack with variation of speed of node in network. It can be observed that the end to end delay in both conditions is varying. AODV can perform in both situation and there is very less effect of node speed in performance.

g. A maximum packet received is the Ratio of received packets that may have been received in the network to the total number of packet sent.

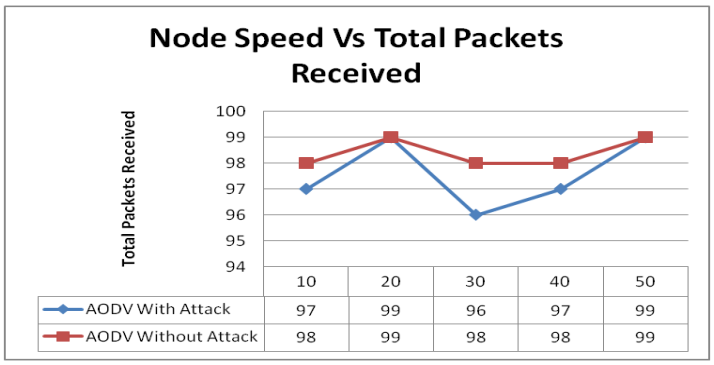


Figure7:- Node Speed Vs Total Packet Received

Figure 7 shows total packet received of AODV in presence and without presence of black hole attack with variation of speed of node in network. It has observed that nodes can receive more packets when network uses AODV without attack. There is much variation in AODV with attack, because nodes in network are move with different speed. Receiver received minimum packets in presence of attack when nodes in network are moving with speed of 30 m/s.

h. Average Jitter effect signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

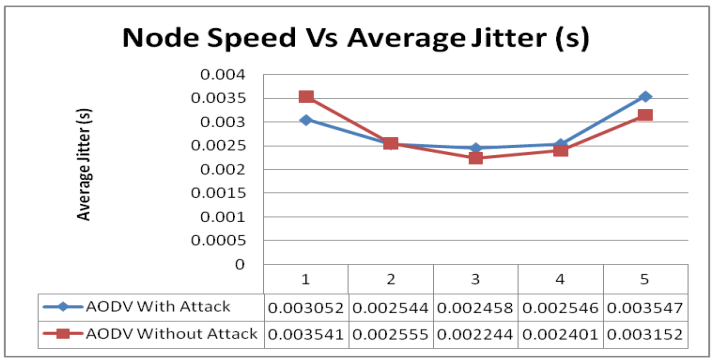


Figure8:- Node Speed Vs Average Jitter

Figure 8 shows average jitter of AODV in presence and without presence of black hole attack with variation of speed of node in network. It can observe that average jitter by AODV is similar in both situations. But most of the time AODV in without attacking situation has less jitter.

VI. CONCLUSION

This paper presents a presents an analysis of AODV routing with and without black hole attack in different scenario in ad hoc network. By different analysis it can be observed in results that AODV can perform better without presence of black hole attack in all situations. If we cannot find similar results as AODV produce without black hole attack than we can predict that there may be an attack on network.

REFERENCES

[1] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network", Ericsson Review, No.4, 2000, pp. 248-263.
[2] G.V.S. Raju and G. Hernandez, "Routing in Ad hoc networks," in proceedings of the IEEE– SMC International Conference, October 2002.
[3] Qualnet Simulator Documentation. "Qualnet 5.0 User`s Guide", Scalable Network Technologies, Inc., Los Angeles, CA 90045, 2006.
[4] A.Boomarani Malany 1, V.R.Sarma Dhulipala 2, and RM.Chandrasekaran 3 "Throughput
and Delay Comparison of MANET Routing Protocols", Int. J. Open Problems Compt. Math.,
Vol. 2, No. 3, September 2009 ISSN 1998-6262; Copyright ©ICSRS Publication, 2009 www.icsrs.
org
[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security
and Privacy, 1540- 7993/04/$20.00 © 2004 IEEE, May/June 2004.

[6] Existing MANET Routing Protocols and Metrics used Towards the Efficiency and Reliability- An Overview Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Ali Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia 1-4244-1094-
0/07©2007 IEEE.
[7] Daniel Lang , "On the Evaluation and Classification of Routing Protocols for Mobile Ad Hoc Networks " 2006.
[8] "Security and Privacy in Location Based MANETs/VANETs" OPNETWORK,
www.ics.uci.edu/~keldefra/manet.htm 2005
[9] Julian Hsu Julian Hsu, Sameer Bhatia, Mineo Takai, Rajive Bagrodia Performance of mobile ad hoc networking protocol in realistic scenario 2005
[10] A Performance Comparison of Routing Protocols for Large-Scale Wireless Mobile Ad Hoc Networks Ioannis Broustis Gentian Jakllari Thomas Repantis Mart Molle Department of Computer Science & Engineering University of California, Riverside 2004
[11] Performance Comparison of MANET Routing Protocols in Different Network Sizes Computer Science Project David Oliver Jörg, 2003
[12] C. Cheng , R. Riley , S. P. R. Kumar , J. J. Garcia-Luna-Aceves, " A loop-free extended Bellman-Ford routing protocol without bouncing effect", Symposium proceedings on Communications architectures & protocols, p.224-236, September 25-27, 1989, Austin, Texas,
United States.
[13] Xin Yu, "Distributed Cache Updating for the Dynamic Source Routing Protocol," IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 609-626, Jun., 2006
[14] M. K. Marina, S. R. Das "Routing performance in the Presence of Unidirectional Links in Multihop Wireless Networks," Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jun. 2002
[15] Charles E.Perkins. Ad hoc Networking, Addison-Wedey, 2001
[16] T. S. Rappaport. Wireless Communications: Principles and Practice. Prentice-Hall, 1996.
[17] A. Lindgren, "Infrastructured Ad Hoc Networks," Proc. 2002 Int'l Workshop on Ad Hoc Networking, Vancouver, August 2002.
[18] J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. Fourth ACM MobiCom, pp. 85- 97, 1998.
[19] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007
[20] Frank Karg, Stefan Schlott, Andreas Klenk, Alfred Geiss, MichaelWeber, "Securing Ad hoc Routing Protocols", 30th EUROMICRO Conference (EUROMICRO'04), IEEE-2004.
[21] Bhavyesh Divecha, Ajith Abraham, Crina Grosan, Sugata Sanyal "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility Models" First Asia International Conference on Modeling & Simulation (AMS'07) : March 2007 pp. 224-229.
[22] D. B. Johnson, D. A. Maltz, Y.-C. Hu and J. G. Jetcheva. "The dynamic source routing protocol for mobile ad-hoc networks". IETF Internet draft, draft-ietf-manet-dsr-04.txt, November 2000.
[23] Performance Comparison of MANET Routing Protocols in Different Network Sizes Computer Science Project David Oliver Jörg, 2003
[24]Rajiv Misra, C.R.Mandal"Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation"0-7803-8964-6/05/$20.00 lEEE 2005
[25] Rama Murti "Wireless Networking" 2008.
[26]D. Djenouri, A. Derhab, and N. Badache. Ad hoc networksrouting protocols and mobility. Int. Arab J. Inf. Technol.3 (2):126–133, 2006
[27]Layuan, Li Chunlin, Yaun Peiyan "Performance evaluation and simulation of routing protocols in ad hoc networks",February 2007, Computer Communication