International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

BEHAVIOUR OF AODV MANET REACTIVE ROUTING PROTOCOL IN PRESENCE OF BLACK HOLE ACTIVE ATTACK USING NETWORK SIMULATOR

Sakhi Jain, M.Tech.Scholar (GGITS Jabalpur) ; Sharda Patel, Astt.Prof. ; Ashok Verma, Assoc.Prof .

Abstract

Mobile Ad-Hoc Network is an interconnected network of mobile devices connected by wireless links moving arbitrarily. They are extremely susceptible to a variety of attacks. One of them is Blackhole.

In this paper, therefore, we focus on analyzing the security of one of the popular routing protocol for MANET the Ad hoc On Demand Distance Vector (AODV) routing protocol. Using different performance metric parameters like Sent packets, received packets, Routed packets, PDF and Packets Dropout using Network Simulator. Our focus is to provide security from the Black hole. Finally the results have been computed and the simulation result shows that increases the black-hole node decreases the AODV activity.

Keywords:

Mobile Ad-hoc Network (MANET), Routing protocol, Ad hoc On Demand Vector Protocol (AODV), Black Hole Attack, Network Simulator(NS2), Packet Delivery Ratio (PDR).

Introduction

MANET is a mobile ad-hoc network which dynamically set up temporary paths between the nodes that are mobile and acts as a router and also hosts that send and receive packets [12]. Once the intended destination is reached by a packet, it replies back to the source by the same route.

Nature of the mobile nodes in MANET makes them extremely undefendable to a variety of security hazards [16]. Routing plays an important role in security of the entire network. Thus operations in MANETs introduce some new security problems other than fixed networks [15].

Figure I. Mobile Ad hoc network (MANET)

In MANET routing protocols are used for communication [3] [7]. They are classified into different categories.

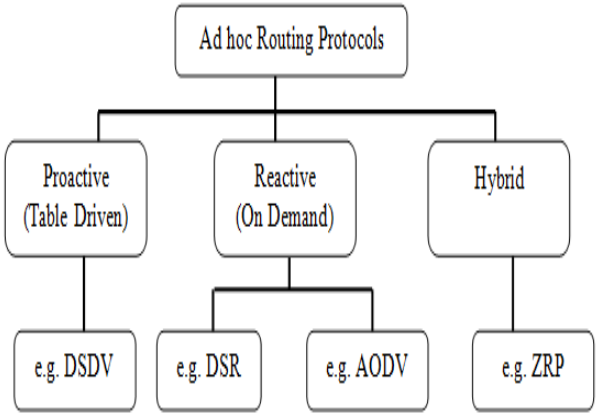

Figure II. MANET Routing Protocols

Proactive Routing Protocol:

Also known as Table-driven routing protocol. Up-to-date routing information is required from each node to all other nodes present in the network.

Destination-Sequenced Distance Vector Routing Protocol (DSDV), Optimized Link State Routing Protocol (OLSR), Wireless routing protocol (WRP) are the type of proactive routing protocol.

Reactive Routing Protocol:

In this the routes are created only when it is desired by the originator. It is also referred as On-Demand Routing Protocol.

Ad-Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing Protocol (DSRP), Temporally Ordered Routing Algorithm (TORA), are some On-Demand Routing protocols.

Hybrid Routing Protocol:

It combines the advantages of proactive routing and reactive routing to overcome the defects of them. The familiar hybrid routing protocols is zone routing protocol (ZRP).

AODV Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a way to the destination in an ad-hoc network [1] [6]. For this all mobile nodes work in cooperation using the routing control messages. The following control packets are used:

Routing Request Message (RREQ):

This message is conveyed by the node who wants a route to the other node

Route Reply Messages (RREP):

This message is unicasted back to the originator of a RREQ if the receiver is either the node using the offered address, or has a valid route to the desired address.

Route Error Messages (RERR):

If in case any link breakage in an active route is found, a RERR message is used to disclose the other nodes about it.

The most distinguishing feature of AODV compared to the other routing protocols is that it makes sure the route to the destination does not contain a loop and is the shortest path.

Black Hole Attack

Black hole attack, is a kind of active attack, it drops the entire outgoing and incoming packet between the source and destination. In this, a malevolent node sends forged routing information, claiming that it has a flawless route to the destination and causes other good nodes to route data packets through it [3] [8] [9].

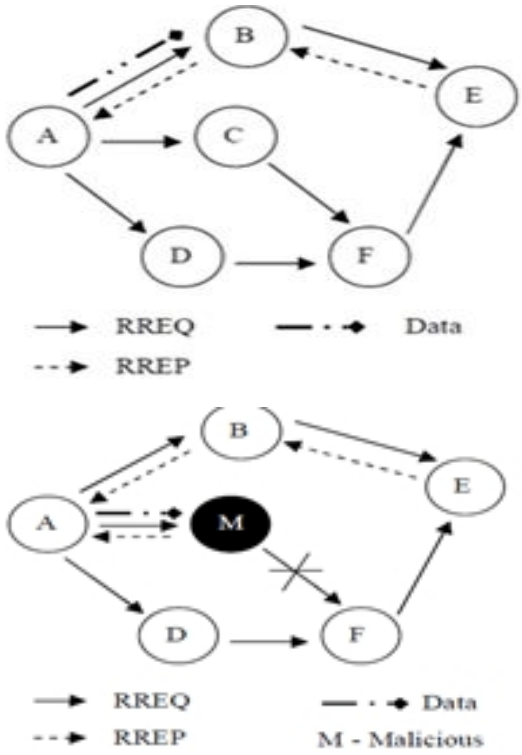

Figure III. Black Hole Attack

As soon as the pernicious node receives RREQ message, without checking its routing table it instantly sends a fraudulent RREP message with a high sequence number and minimum hop count to the source so that it can make an entry in its routing table [15].

The reply is sent by the pernicious node before any other node. In this way it establish a link with the source and in-

ISSN:2319-7900

stead of promoting further it starts dropping the data sent from the source for the destination [2].

Proposed System

In this Paper Black Hole attack is simulated in wireless ad-hoc networks by using NS-2.34 simulator [6] [14]. Firstly a new Black Hole protocol is added into the NS-2. It is done by customizing an existing AODV protocol using C++, to simulate the Black Hole attack and compare the network performance with and without black holes in the network. As expected, network performances degrade due to black hole attack.

Implementation of Black Hole Attack

1. All the files present in aodv except packet.h is duplicated and named as blackaodv.

```
blackAODV {
set ragent [$self create-blackaodv-agent $node]
}
Simulator instproc create-blackaodv-agent { node } {
set ragent [new Agent/blackAODV [$node node-addr]]
$self at 0.0 "$ragent start" # start Messages
$node set ragent_ $ragent
return $ragent
}
```

2. Then "\tcl\lib\ ns-lib.tcl" file is customized for the coding of the agents. When the nodes use blackaodv protocol, this agent is scheduled at the beginning of the simulation and is assigned to the nodes that are going to use the blackaodvprotocol.

3. Secondly "*makefile*" in the root directory is prepared.

```
blackaodv/blackaodv_logs.o
blackaodv/blackaodv.o \
blackaodv/blackaodv_rtable.o
blackaodv/blackaodv_rqueue.o \
```

4. So far, a new protocol labeled as blackaodv is implemented. But implementation of Black Hole behaviors has not yet been done. To add Black Hole behavior some changes are made in blackaodv/blackaodv.cc C++ file.

Experimental Setup

The simulation is performed using NS-2 (v-2.34) network simulator. It provides faithful implementations of the different network protocols. The number of simulation parameters which can be varied, are shown in below table.

Parameter	Value
Simulator	NS - 2.34
Simulation time	100 s
Number of nodes	10,20,30
Number of black hole nodes	2,4,6
Terrain area	500m x 500m
Routing Protocol	AODV
Packet size	512
Traffic model	CBR

Table I. Simulation Parameters

Result and Analysis

Various types of network contexts are considered to measure the performance of a protocol. These contexts were notified by customizing the below mentioned parameters in the simulation.

Network Size
- Number of Black Hole nodes
- Traffic Load

A. For Two Black Hole Nodes

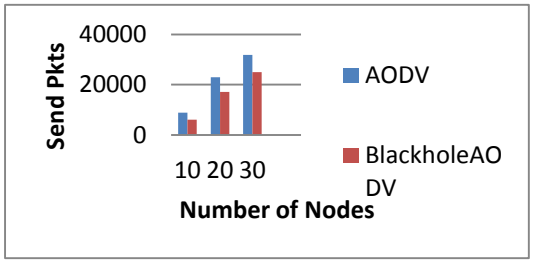

Figure IV (a)

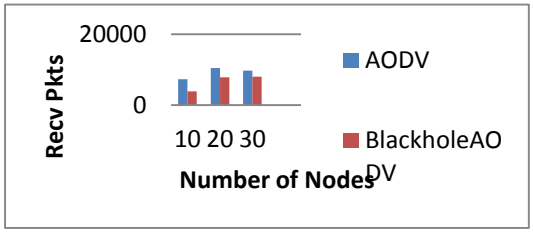

Figure IV (b)

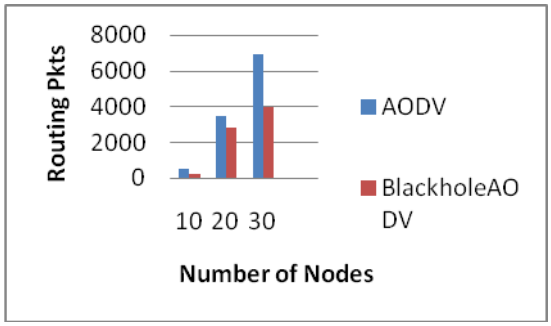

Figure IV (c)

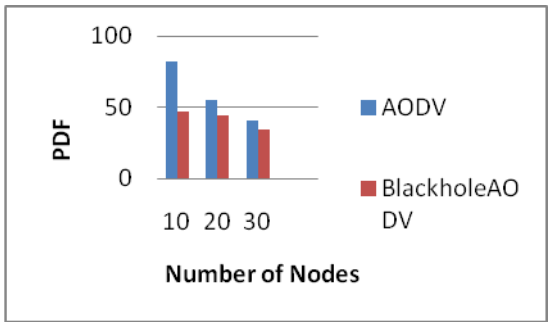

Figure IV (d)

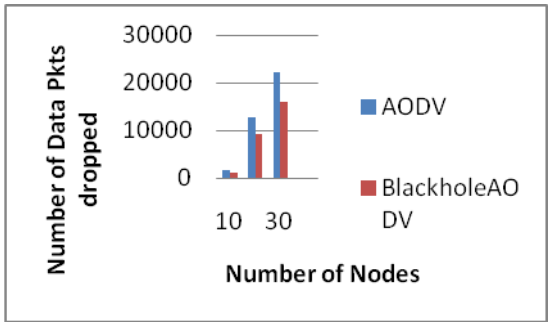

Figure IV (e)

All the above performance metric parameters are simulated and tested to see the effect of generated packet, received packet, routing packets, PDF and number of packets dropped in AODV when there are two Black Hole nodes.

B. For Four Black Hole Nodes

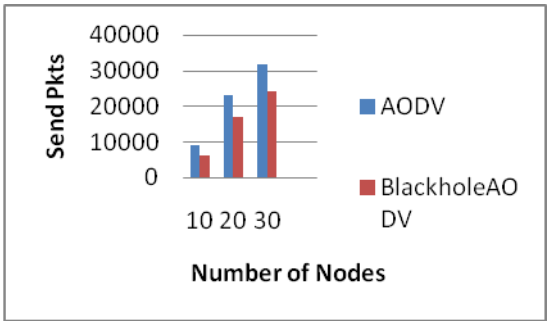

Figure V (a)

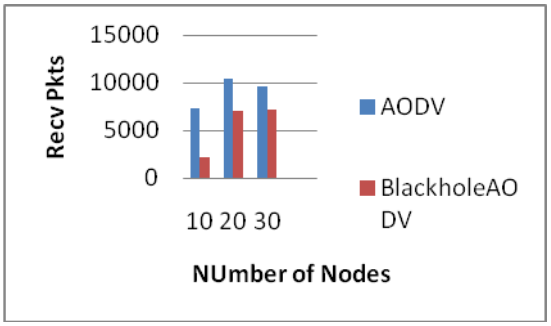

Figure V (b)

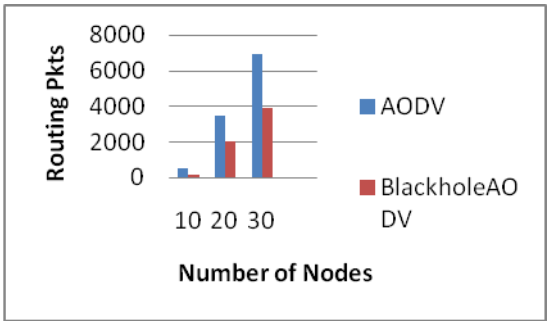

Figure V (c)

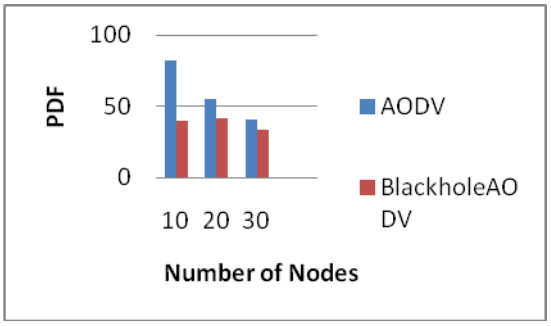

Figure V (d)

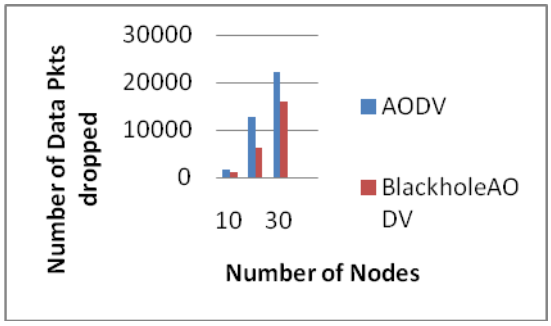

Figure V (e)

All the above performance metric parameters are simulated and tested to see the effect of generated packet, received packet, routing packets, PDF and number of packets dropped in AODV when there are four Black Hole nodes.

C. For Six Black Hole Nodes

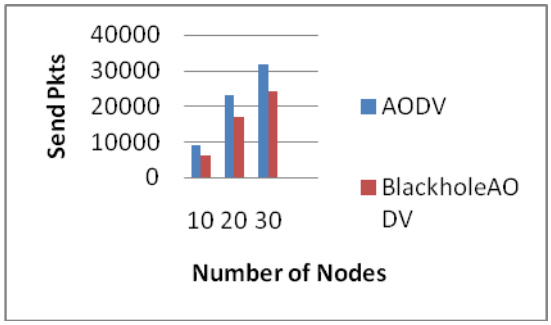

Figure VI (a)

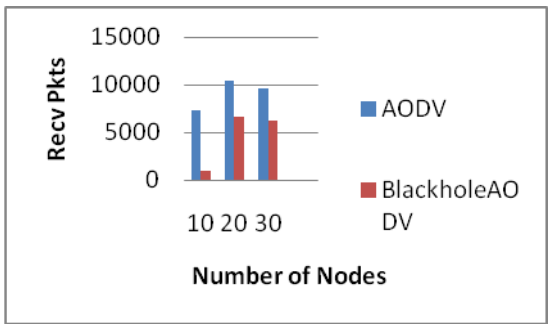

Figure VI (b)

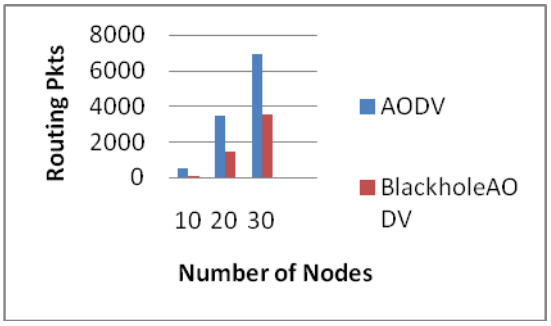

Figure VI (c)

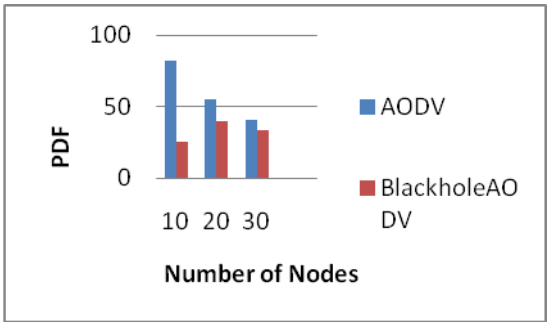

Figure VI (d)

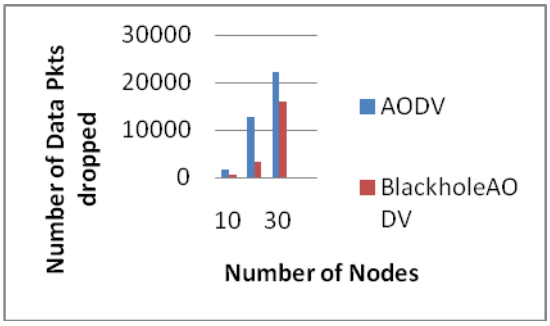

Figure VI (e)

All the above performance metric parameters are simulated and tested to see the effect of generated packet, received packet, routing packets, PDF and number of packets dropped in AODV when there are six Black Hole nodes.

Conclusion

The effect of the Black Hole attack was analyzed in an AODV protocol. Simulation results shows that on increasing the number of black hole nodes like 2, 4 and 6 packet loss is increased in the ad-hoc network. Initially there is no data loss in the AODV network but on introducing the black

ISSN:2319-7900

hole nodes the data loss is high and network performance degrade.

References

[1] Mangesh Ghonge and Prof. S.U. Nimbhorkar "Simulation of AODV under Blackhole Attack in MANET", International Journal of Advaced Research in Computer Science and Software Engineering Vol 2, Issue 2, Feb 2012

[2] Arti Sharma and Satendra Jain " A Behavioral study of AODV with and without Blackhole Attack in MANET", International Journal of Modern Engineering Research Vol 1, Issue 2, 2012

[3] Chandni Garg, Preeti Sharma and Prashant Rewagad " A literature survey of black hole attack on AODV routing protocol", International Journal of Advancement in Electronics and Computer Engineering Vol 1, Issue 6, Sep 2012

[4] Monika Roopak , Dr Bvr Reddy "Performance Analysis of AODV Protocol under Black Hole Attack" International Journal of Scientific Engineering Research 2011.

[5] Harris Simaremare and Riri Fitri Sari "Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious attacks". In IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.

[6] Nisarg Gandhewar, Rahila Patel "Performance Evaluation of AODV protocol in MANET using NS2 Simulator" International Journal of Computer Application 2011.

[7] Fan-Hsun Tseng, Li-Der Chou1 and Han- Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011.

[8] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das "Security Measures for Black Hole Attack in MANET: An approach", International Journal of Engineering Science and Technology, Vol 3, No. 4 Apr 2011.

[9] Anu Bala, Raj Kumari, Jagpreet Singh "Investigation of Blackhole Attack on AODV in MANET" Journal of Emerging Technologies in Web Intelligence 2010.

[10] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks" Proceedings of the International Multiconference of Engineers and Computer Scientists 2010.

[11] Latha Tamilselvan, Dr V Sankaranarayanan, "Prevention of Blackhole Attack in MANET". 2nd International Conference on Wireless Broadband and Ultra Wideband Communications India, 2007.

[12] T. Franklin, "Wireless Local Area Networks", Technical Report http://www.jisc.ac.uk/uploaded_documents/ WirelessLANTechRep.pdf. 25 July 2005.

[13] Hao Yang, haiyun Luo, Fan Ye , Songwu Lu, Lixia Zhang , " Security in mobile ad hoc networks : challenges and solutions", Wireless Communication , IEEE , Vol 11, No. 1, pp 38-47, Feb 2004.

[14] Network Simulator Official Site for Package Distribution, web references, http://www.isi.edu/nsnam/ns.

[15] H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, Oct. 2002.

[16] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, Oct 2002.