Simulation study of Collaborative Attack on Wireless Mobile ADHOC Network with AODV Routing Protocol on MANET

1Gurpreet Kaur, 2 Deepinder Kaur Dhaliwal, 3 Neha Soni
1CSE Dept, Desh Bhagat University, MandiGobindgarh,Punjab , India
Preetcheema34@gmail.com
2HOD CSE Dept, Desh Bhagat University, MandiGobindgarh,Punjab , India
Deepinderdhaliwal1989@yahoo.com
3CSE Dept, RIMT, MandiGobindgarh,Punjab , India
ruheesoni@yahoo.co.in

Abstract: **This is a preliminary requirement of a communication among the cooperative nodes in a network is establishing by Manet. There is no need of any Infrastructure to Communicate in Mobile ADHOC. In this paper we can analyze the simulation results by applying the Black hole and wormhole attack as a collaborative attack on MANET using ADOC on demand distance vector (AODV) routing protocol in . we get the results what kind of impacts are drawn with or without collaborative attack on MANET and analyze the how much performance degrade and packet lose ratio and average end to end delay with or without collaborative attack .the simulation is carried on opnet and the simulation results are analyzed on various network performance matrices.**

Keywords: **wormhole attack, black hole attack, MANET, AODV routing protocol, OPNET tool.**

I. Introduction

Mobile ADOC is a collection of mobile devices that works with some fixed or mobile work stations without any central Network authority or infrastructure. By the packet forwarding the mobile devices can easily communicate with each other. Due to no fixed infrastructure these mobile devices can easily join or leave the network. In a connectivity of nodes in a network either a wired or wireless channel are used. The nodes act as host or router in manet network for route to discover or to forward the packets to the other nodes in the network.

Some special characteristics of MANET are open medium, dynamic topology, lack of central management, cooperative algorithm .there are exposed a numbers attack in a open environment and collaborative attack is one of them.

In this paper we analyze the simulation study of packet data dropped and show the comparative study of performance evaluation of MANET using the AODV routing protocol with and without collaborative attack on MANET.

II. Wireless Communication

Wireless communication is becoming more popular today between mobile users. Wireless such as modem and Lan are the recent technological uses in laptop computers and wireless data communication devices that lead to lower prices and higher data rates, which are the two main reasons that increase the growth of mobile computing . There are two types of approaches for enabling wireless communication between two hosts. First approach leads to existing cellular infrastructure of network which carry the data and voice.Second phase tends to mobile ADHOC network in which all the participated nodes can communicate with each other. the ad-hoc approach. Ad-hoc networks as compared to traditional cellular systems show many advantage. These advantages include:

- On demand setup
- Fault tolerance
- Unconstrained connectivity

There is no pre-established infrastructure and can therefore be deployed in places with no infrastructure.

III. Overview of AODV routing protocol

The AODV routing protocol is a on demand routing protocol type. Each nodes can be consist the routing table and the freshness of nodes may be defined by sequence no. each node can receive the control packet then routing table can become update by using the sequence no of each nodes. AODV routing protocol establish the route discovery phase and route maintenance phase.

1. *Route discovery phase*:

Whenever a source node send a request message (RREQ) to a destination. And there is not a proper route in a routing table for broadcasting the packet to source to the destination. Then these RREQ message can be broadcasting to all the neighbor nodes each node can receive the RREQ message and creates or update reverse path to source node in a routing table. If these nodes cannot find the exact destination a routing table then source node can rebroadcast the RREQ message. The RREQ can be flooded from source to destination and create or

update the reverse path route. Once the RREQ message reach at the exact source node can receive the RREP message from the destination node then it will start the data packet forwarding. In this way communication is held between the source and the destination.

2. Route maintenance phase:

In route maintenance phase for a connectivity of the various nodes the "hello" packets are broadcast periodically. Destination node can broadcast the RREP message with TTL=1 as a "HELLO" message. When the packet cannot be received in a second from the neighbor then it became assume that link is break among the neighbor. To know which link is break its depend upon the acknowledgment of MAC layer of neighbor The braked link requires a fresh route to destination node for a local repair which is detect by MAC layer.

In the protocol newly developed route update procedure with combined metrics of delay, hop count and disjointness, each intermediate node deliberately selects multi-path candidates while contributing to suppression of unnecessary routing packets. There are a two methods which can be specify by the AODV routing protocol in which one of them is based upon hop count minimization. In it when the RREQ and RREP message are forwarded and reversed are delayed both the route are updated and data packets are show the less Hop Count.

Second method is based upon the delay minimization principle. This principle can be defined as when the RREQ/RREP message can be accepted according to their arrival order and there is no need of unicasting of data packets.

Modified AODV: the extension of the AODV routing protocol can be done in two types of control packets that is RRDU (reliable Route Discovery Unit) And RRDU-REP (reliable Route Discovery Unit –reply).
Two Fields of AODV Routing protocol: There are two fields of AODV routing protocol i.e. RREQ field (Route Request field) And RREP (i.e Route reply field).

3. Route request field:

RREQ Field

Sourc e Add	Source Seq-------uence	Broadcast id	Destinati on Add	Destinati on Sequence	Hop Count

IV. COLLABORATIVE ATTACK

Collaborative attacks may attacks on a running process and it may disturb the running process in a network. In this paper we analyze collaborative attack on manet as using Black hole and Wormhole attack and see the impact of the collaborative attack on wireless network on MANET.

V. Multiple node attacks:

1. Black hole attack:

A black hole attack occurs when a malicious node pretend as original node with fraudulent intentions as the destination node The malicious node may generate unwanted traffics and usually discards packets received in the network .Whenever black hole node can attack on one or multiple nodes in a network then is became known as collaborative black hole attack.

In a black hole attack, the malicious node presents itself as having the shortest path to the node and make fraudulent image, making it easier to intercept the message. To achieve this, the malicious node waits and tries to get the replies from nearby nodes in order to discover a safe and valid route [9].

In the above example S is the source node and D is representing the Destination node .For data sending source node to destination node. S node broadcast the RREQ message to its neighbor. in the above example B1 and B2 nodes are represent the Black hole nodes and these nodes can receive the RREQ message from S node and these malicious nodes can send back the RREP message to the Source node .these malicious nodes can claim to the shortest path to the destination node D. then Source node start forwarding the data packets. BI is a Black hole can receive this data packet Bi may drop the data packet or may be forward to the second malicious node B2. And there is no data which can reach at the destination at D node.

2. Worm hole attack:

In wormhole attack attacker degrade the network and provides two choke-points that are used. False impressions are used in creating these choke-points with two or more nodes joint together In other words, wormhole attack creates a tunnel that records traffic data (in bits or packets) at one network place and channels them to another place in the network. This kind of attack is usually against many ad hoc routing protocols and the attacker is hidden at higher layers; thus the wormhole and both colluding attacker nodes at each choke-point of the wormhole are invisible in the MANET route. In the above example the worm hole attack can be exist in a clouding network tunnel. It may include at least two malicious node in a tunnel of network which may

read all the data packets forwarding from the previous participating nodes .node 5 and node 6 are the malicious nodes (wormhole nodes) in a tunnel and these nodes can analyze the data and by using the wired link or a long range medium it became tamper the networks.

VI. Simulation

In opnet a network have created with AODV protocol & checked that how much packet data dropped in AODV protocol. For this a simple Scenerio of network is created with the AODV protocol is shown in Fig 1 and various parameters. By using parameters this network will help to find out, how much data is dropped by using AODV protocol and how it will help to improve the performance of the network. In this 11 nodes are used in Manet network nodes. Which is connected with topology 802.11.

Fig 1 MANET Network with AODV Protocol

The result of scenario 1 is shown in fig 2 in which the total packet dropped in the network.

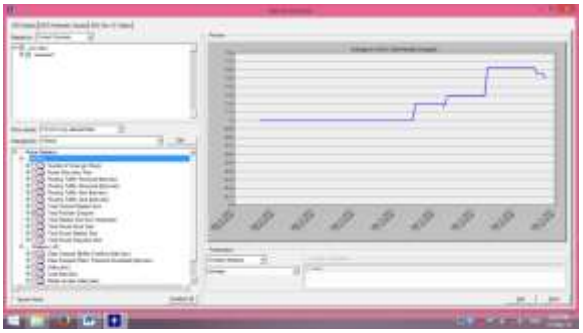

Fig 2 Total packet dropped using AODV Protocol

As it can be seen from fig 3, the node 4 acts as a Black Hole node in scenario 2. The node 4 may generate unwanted traffics and usually discards packets received in the network In Fig 4 it is been shown that how the packet dropped will be increased.

Fig 3 MANET Network with Black Hole Attack

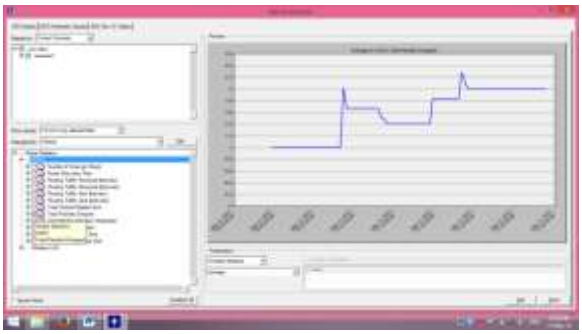

Fig 4 Total packet dropped in Black Hole attack

The comparison of the results of both the scenarios it has been finding out that the total packet dropped increased on applying the black hole attack on the nodes. The difference between both the scenarios is shown in Fig 5. So the data can be protected from the attackers by applying Protection scheme on the Protocols.

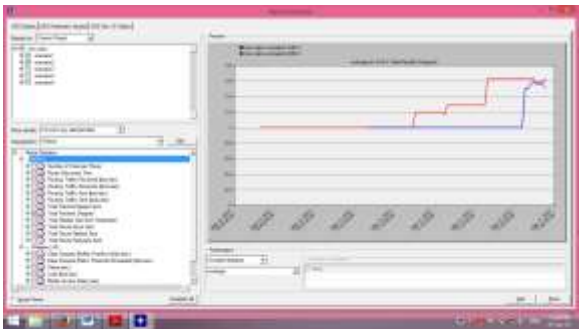

Fig 5 Comparison between Total Packet Dropped manet network, Network with Black Hole

As it can be seen from fig 6 , the node 3 & 4 acts as a Worm Hole nodes in scenario 2. The node 3 & 4 in which the attacker provides two choke-points that are used to degrade the network or analyze traffic as preferred any time. In Fig 7 it is been shown that how the packet dropped will be increased.

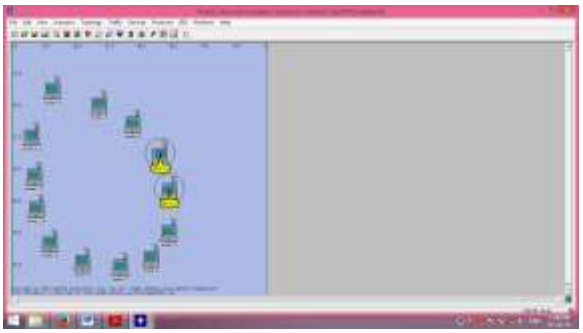

Fig 6 MANET Network with Worm Hole Attack

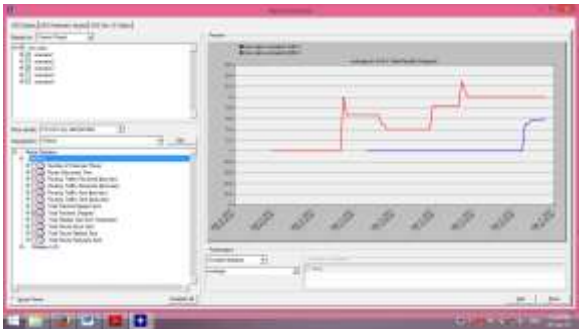

Fig 7 Total packet dropped in Worm Hole attack

The comparison of the results of both the scenarios it has been find out that the total packet dropped increased on applying the black hole attack and Wormhole on the nodes. The difference between both the scenarios is shown in Fig 8. So the data can be protected from the attackers by applying Protection scheme on the Protocols.

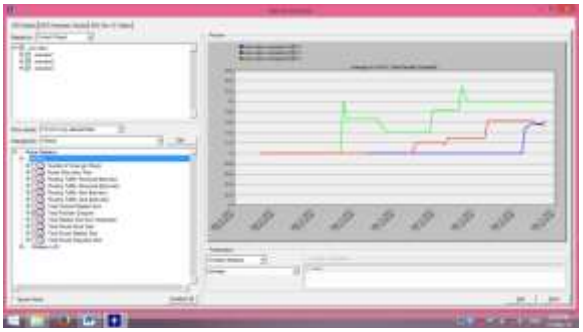

Fig 8 Comparison between Total Packet Dropped manet network,Network with Black Hole and Wormhole

By changing AODV parameters and increasing transmission range. Network performance should improve which is shown in Scenerio fig no 9

Fig 9 Improved MANET Network with AODV Protocol

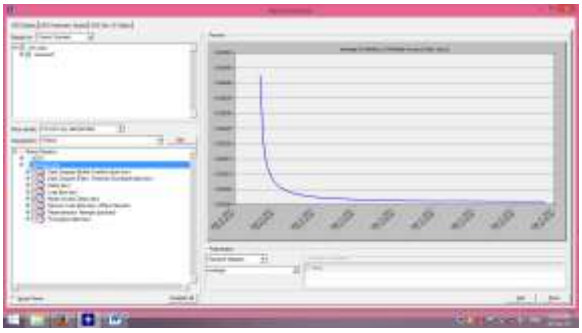

Fig 10 Improved delay MANET Network with AODV Protocol

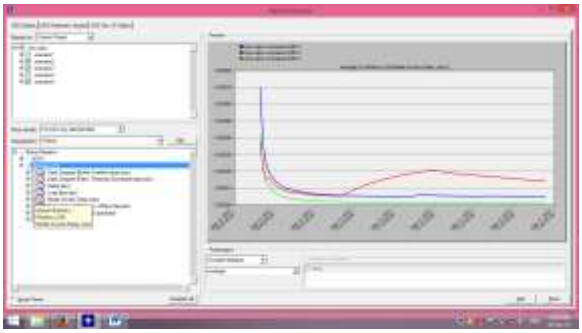

Fig 11 Comparison between Improved delay MANET Network with normal manet Network using AODV Protocol

VII. Conclusion

In this we seen how Black hole and Wormhole attack degrade the network performance by increasing total packet dropped. In Future Scope There are various Prevention Methods in the AODV to protect it from the Black Hole and Wormhole Attack.

References

1. Singh, Pooja Nagpal, Sukhvir Singh "Behavior of Reactive Routing Protocols for MANETs: a Review" International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181 Vol. 3 Issue 12, December-2014.
2. Rasha T. K, Shwetha Vincent," Efficient Routing Protocol For Mobile Ad Hoc Networks"International Journal of Engineering Research & Technology ISSN: 2278-0181 Vol. 2 Issue 3, March – 2013
3. IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE

Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York.

4. Shalini Midha,Naveen Hemrajani"Performance Analysis of AODV & OLSR for MANET"International Journal of Engineering Research & Technology ISSN: 2278-0181Vol. 2 Issue 1, January- 2013
5. Anjaly Joy et al "Black Hole Attack & its Mitigation Techniques in AODV & OLSR", International Journal of computer Science &Technology , Vol 4, No.6, Pg. 740-745, June-2013
6. Er. Gurjeet singh " Performance And Effectiveness Of Secure Routing Protocols In Manet", Global Journal Of Computer Science And Technology. ISSN 0975-4172 Volume 12 Issue 5 Version 10 March 2012

[7] E.Alotai i and ukherjee survey on routing algorithms for wireless d- oc and mesh networks Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56,no. 2, pp. 940–965, October 2011.

[8] M. Zhang and hong erformance comparison of lat and luster- ase dierarchical docouting with ntity and roup o ility in Proc. of IEEE Communications Society conference on Wireless Communications & Networking, Budapest, Hungary, 2009 pp. 2450-2455.

