Simulation & Analysis of Routing Protocols of MANET -A Review

Sharandeep Kaur[1] Shailesh Pathak[2]
[1,2]JCDM College of Engineering Sirsa, Haryana, India

Abstract— In this paper, we describe a simulation and analysis study of Wireless network in routing protocols using MANET. AODV (Ad-Hoc On-Demand Distance Vector Routing) Self-configuring network of mobile routers connected by wireless links .In Black hole attack on AODV no of nodes a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears . At the advanced type of AOMDV protocol are used AOMDV(Ad-Hoc On-Demand Multiple Routing) - a multipath extension to AODV multiple loop-free and link-disjoint paths. AOMDV as better than AODV. The simulation result AOMDV protocols packet data send energy consumption and at a same time so many packet deliveries. These are different parameter are calculate Throughput, PDR (Packet Delivery Ratio), and measured the End to End delay on different network scenarios. Measure the protocols with different packet size and calculate the Energy Consumption. This work will be done with help of the ns-2 simulator. (Network Simulator 2.34) .

Keywords: Ad-Hoc On-Demand Distance Vector Routing (AODV), Ad-Hoc On-Demand Multiple Routing(AOMDV) , ns-2 simulator, MANET.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) is an infrastructure less wireless network in which nodes do not required any base station for communication amongst them. Each node acts as router between source and destination. The nodes are free to move in any direction independently making the topology dynamic. MANETs has various applications (1) in military application for decision making in the battlefield and rescue operations, (2) in public application such as conferencing and disaster relief.

The design of protocols important issue is AODV on Black hole Attack .As compared AODV protocols in enhancement protocols AOMDV over the AODV protocols better performance in AOMDV. The study of routing protocols and the Attacks. The important issue of create a scenarios network no. of nodes AODV then the Black hole Attack on AODV. Therefore the sending packet data dropping at the bottle neck and they are lost of energy [1]. So in this paper we use the advanced protocols AOMDV in a packet delivered. These are parameter is calculating Throughput, PDR (Packet Delivery Ratio), and measured the End to End delay on different network scenarios. Measure the protocols with different packet size and calculate the Energy Consumption.

II. MANET ROUTING PROTOCOLS

MANET routing protocols are so many type of protocols AODV, DSDV, DSR, TORA. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an inter-network. The later concept is called as packet switching which is straight forward, and the path determination could be very complex[3]. When the using AODV protocol, Black hole Attack on AODV, and other protocol is AOMDV explained in this paper .

Ad-Hoc On-Demand Distance Vector Routing (AODV)

The mobile networks are indispensable for the communication between different types of mobile devices, allowing that the users should have access still when they move to and from without need to realize a new connection. [3]. Mobile device communicate in peer-to-peer fashion. Self-organizing network without the need of fixed network infrastructure .Multi-hop communication. Decentralized, mobility-adaptive operation. Route Requests (RREQ) are flooded on demand .When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source. Different type of Routing Protocols of MANET.

- Active
- Reactive
- Hybrids

AODV assumes symmetric (bi-directional) links. When the intended destination receives a Route Request, it replies by sending a Route Reply Route Reply travels along the reverse path set-up when Route Request is forwarded.

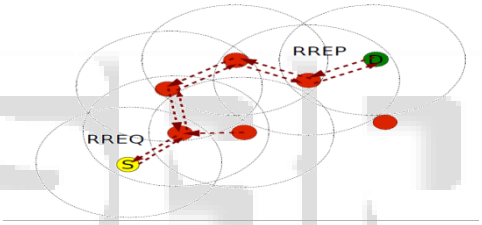

Fig. 1: Example: Route Discovery AODV

The principal characteristic is that the nodes only exchange information of control, when they want to initiate a communication with another node.[3] . creating nodes then the using the different network scenarios simulation the ns

III. CHARACTERISTICS

- Only when it needs to communicate, the process of discovery of route begins.
- Major time in the delivery of packages.
- Low utilization of resources and it introduces few overcharge in the network due to the fact that it doesn't do a constant update of routes.
- It supports a locally table of route ring for the already known destinies.
- It only supports the use of unidirectional links.
- It uses HELLO messages (they are used to support the information of local connectivity of a node to other one).
- They use a unique number of sequences for every destination.
- AODVs functioning depends on that every node keeps his own number of sequence updated.

IV. BLACK HOLE ATTACK ON AODV

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter

and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components.

The Black-Hole node separates the network into two parts. Few strategies to mitigate the problem:

- Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found.
- Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

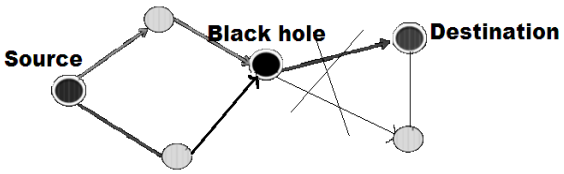

Fig. 2: Black Hole Attack

A. Active Routing Attacks

The passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network. A malicious node may perform an active attack in order to disable a service or in order to conserve energy. An active attack may either being directed to disrupt the normal operation of a specific node or target the performance of the ad hoc network as a whole. In this section the most important active attacks are presented that can be easily be performed by an internal node against the utilized ad hoc routing protocol .

B. Routing Overflow

In a routing table overflow attack the attacker attempts to create routes to non-existing nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing protocols are more vulnerable to this attack, since they attempt to create and maintain routes to all possible destinations**.** . To implement this attack in order to target a reactive protocol like AODV is slightly more complicated since two nodes are required. The first node should make a legitimate request for a route and the malicious node should reply with a forged address.

This method improves the routing update process as well as analyzing the receive reply control messages (RREP) to isolate black hole malicious nodes. This method assumes the destination node is reachable by route request and normal black hole characteristic is high destination sequence number carried in route reply.[5] The no. of nodes are create a area Source to Destination nodes a fix of route in packet sending data. When attack the fix of nodes in routing path then back hole attack if we see the at a bottle neck of nodes packet drop tail. These are packet other node deliver. And the route is change and don't energy consumption or packet delay on the Destination nodes as shown in figure (2).

Black hole attack and provides routing security in AODV by purging the threat of black hole attacks. Different types of attacks. The classification of attacks. The categorized the presently existing attacks into two broad categories:

- DATA traffic attacks
- CONTROL traffic attacks.

where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers [5]

Ad hoc on-demand multipath distance vector routing (AOMDV)

In each route discovery, find multiple routes between source and destination. Use alternate routes on a route failure. New route discovery needed only when all routes fail. Fewer number of route discoveries. Reduction in delay and routing overhead.

1) AOMDV multipath extension to AODV

A multiple loop-free and link-disjoint paths.

2) AOMDV performance relative to AODV

- more than factor of two improvement in delay.
- about 30% reduction in routing load.

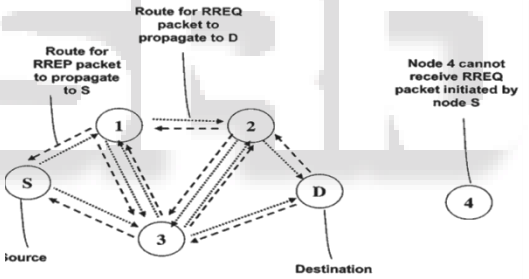

Fig. 3: Ad hoc on-demand multipath distance vector routing (AOMDV)

The protocol guarantees loop freedom and disjoint of alternate paths.[6] Performance comparison of AOMDV with AODV shows in figure (3) that AOMDV is able to effectively cope with mobility-induced route failures.[6]. In the AOMDV protocol in the enhancement over the AODV . when it use of as compared to the better than AOMDV. These are more Security and the many path of packet source to Destination packet deliver. The no of nodes use as shows in figures(3). The source for RREP packet to propagate to S. then the nodes 1 to node 2 is route for RREQ packet to propagate to D. same as that the node 1 or node 2 packet send at that same time node 3. The node 4 cannot receive RREQ Packet initiated by node S.

C. Route maintenance

Route maintenance in AOMDV is a simple extension to AODV route maintenance. AOMDV also uses RERR packets. A node generates or forwards a RERR for a destination when the *last* path to the destination breaks. AOMDV also includes an optimization to *salvage* packets forwarded over failed links by re-forwarding them over alternate paths. The timeout mechanism similarly extends

from a single path to multiple paths although the problem of setting proper timeout values is more difficult for AOMDV compared to AODV. With multiple paths, the possibility of paths becoming stales more likely. But using very small timeout values to avoid stale paths can limit the benefit of using multiple paths. we use a moderate setting of timeout values and additionally use HELLO messages to proactively remove stale routes. Thus, the timeouts in the current version of AOMDV primarily of link behavior in ad hoc networks.

Table. 1: AOMDV Route

Type	Reversed	Last hop	Hop count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			

V. PROTOCOLS OF PARAMETERS

A. Energy Consumption

Energy efficiency is a way of managing and restraining the growth in energy consumption. Something is more energy efficient if it delivers more services for the same energy input, or the same services for less energy input.[1].

Transmitted Energy

Tx Energy = (330*5*Packet Size)/2x106

Receiving Energy

Rx Energy = (230*5*Packet Size)/2x106

Total energy consumed = Initial Energy – Energy left

B. Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections. No. of Packets send by network v/s No. Of packets generated by source.

C. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

$$PDR = S1 \div S2$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

D. End to End Delay

The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination

$$Avg.\ EED = S/N$$

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

VI. CONCLUSION

In this paper we have studied the performance analysis of the routing protocols i.e. AODV, AOMDV using ns-2 simulator from the various authors described in the above 802.11 network. In this paper, we calculate the packet delivery ratio, throughput, packet Loss and time delay for AODV, AOMDV routing protocols . When the various nodes Black hole Attack on AODV.

REFERENCES

[1] Dhiraj Nitnaware, Ajay Verma, "Energy Evaluation Of Two On Demand Routing Protocol Under Stochastic Traffic" 978-1-4244-2746-8/08/$25.00©2008IEEE 2008

[2] Impact of Topology Control and Traffic Models Performance on Mobile Ad Hoc Wireless Routing Protocol (Lawal Bello, Panos Bakalis,) 978-1-4673-5836-1//11/$26.00 ©2011 IEEE

[3] Analysis of QoS parameter in AODV a DSR in mobile Ad Hoc networks (Liliana Enciso Quispe and Luis Mengual Galan,).

[4] An Optimized Ad-hoc On-demand Multipath Distance Vector (AOMDV) Routing Protocol(YuHua Yuan, HuiMin Chen, and Min Jia) 0-7803-9132-2/05/$20.00 ©2005 IEEE.

[5] Mitigation of Black hole for AODV (Ad hoc On Demand Distance Vector) (Ms. Bhumi Jani1, Prof. Hitesh Patel2, © 2013, IJCSMC All Rights Reserved)

[6] Ad hoc on-demand multipath distance vector routing Mahesh K. Marina1,and Samir R. Das Wirel. Commun. Mob. Comput. 2006; 6:969–988

[7] Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Simulation Implementation and Evaluation (Hesiri Weerasinghe and Huirong Fu, Member of IEEE) International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008

[8] M. X. Cheng, M. Cardei, X. Cheng, L. Wang, Y. Xu, and D.-Z. Du, "Topology control of ad hoc wireless networks for energy efficiency," Proc. IEEE, vol. 53, pp. 1629–1635, Dec. 2004.

[9] A Survey on Energy Efficient Routing Techniques in Wireless Sensor Networl< (Md. Atiqur Rahman*, Shahed Anwar**, Md. I1eas Pramanik*, Md. Ferdous Rahman) January 27 - 30. 2013 ICACT2013, ISBN 978-89-968650-1-8

[10] L. Hu, "Topology control for multi hop packet radio networks," Proc. IEEE, vol. 41, pp. 1474–1481, Oct. 1993

