Performance Evaluation of Routing Protocols in MANETs under Wormhole Attack

[1,]Pardeep Kaur, [2,] Deepak Aggarwal

[1,]M. Tech Student , [2,] Assistant Professor

[1,2],Department of CSE & IT, BBSBEC, Fatehgarh Sahib, Punjab, India

Abstract

Mobile Ad-Hoc Network is a group of wireless mobile nodes connected to each-other without any central administrator. Nodes can move from one place to another in the network or may leave or join the network at any time. Due to this the topology of the network changes rapidly. So the routing protocols are required that can adopt the frequent changes in the network topology. Due to the absence of central administrator the MANETs are vulnerable to attacks. In this paper comparison of reactive protocols i.e AODV and DYMO has been done under three types of wormhole attack. Performance is measured with metrics like Packet Delivery Ratio, Average End-to-End Delay, Throughput and Jitter by varying the number of nodes.

Keywords-AODV, DYMO, MANET, Wormhole

1. Introduction

Mobile Ad-Hoc Network is a group of wireless mobile nodes connected to each-other without any central administrator. The nodes can leave or join the network at any time. Nodes act as routers that relay packets generated by other nodes to their destination [Jeroen Hoebeke et al., 2006]. Due to the movement of nodes the topology of the network changes rapidly. The nodes which are near to each other or within each other’s radio range can communicate directly. But nodes which are far away they use intermediate nodes to send data. MANETs has advantages like Simple, cheap and fast setup of networks, more robust concerning failure of single component due to decentralized structure because of these they are used in many applications like wireless sensor networks, rescue operations, sports events and conferences etc.

2. Routing Protocols

Proactive protocols are also known as table driven protocols. In these protocols each node maintains a route in their routing table to all the destination nodes in the network. Due to that, routes are discovered for every mobile node of the network, without any request for communication by the hosts [Gurjinder Kaur et al., 2011]. The routing tables are updated periodically or when a change occurs in the network topology. Some of proactive protocols are DSDV, OLSR and STAR. Reactive protocols are also known as on-demand routing protocols. In these protocols a route is only discovered when source node want to send data to the destination node. Source node broadcast a route request message to find a route to the destination. Some of the reactive routing protocols are DSR, AODV and DYMO. Due to the random movement of nodes, the network topology becomes unpredictable and changes rapidly. In order to find the most adaptive and efficient routing protocols for dynamic MANET topologies, the behavior of routing protocols need to be analyzed at varying node speeds, network size, number of traffic nodes and node density [Fahim Maan et al., 2010].AODV and DYMO routing protocols are used in simulation.

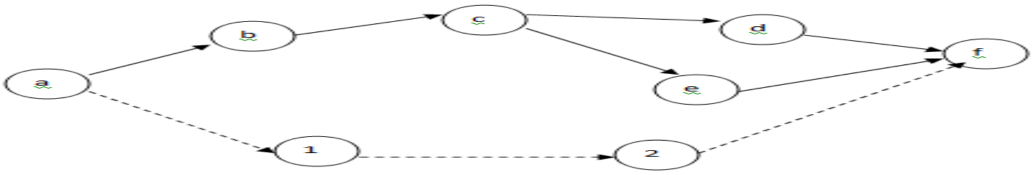
2.1 AODV

Ad-hoc on–demand distance vector is a reactive routing protocol. This property implies that it requests a route when it needs one and the nodes which do not want to take part in active communication, need not to maintain routing tables. AODV uses the sequence number to find fresh routes. AODV has two basic operations: route discovery and route maintenance. AODV uses RREQ, RREP and RERR messages to find and maintain the routes.In route discovery , when a source node desire a route to the destination node for which it does not have a route, it broadcast a route request (RREQ) message in the network. RREQ message contains source IP address, destination IP address, sequence number, hop count and broadcast ID. A neighbor receiving a RREQ may send route reply (RREP), if it is either the destination or if it has unexpired route to the destination. When destination node send a route reply (RREP) message to the source node, a forward path is formed. Now source node will send the data through this path.In route maintenance, when a link breakage in an active route is detected, the node notifies this link breakage by sending a route error (RERR) message to the source node [Dong-Won Kum et al., 2010] . The source node will reinitiate the route discovery process if it still has data to send.

2.2 DYMO

DYMO is a successor of AODV. It is a combination of AODV and DSR routing protocols. Similar to AODV, DYMO has two basic operations, route discovery and route maintenance. In route discovery, the source node broadcast a RREQ message throughout the network to find the destination node. During this process, each intermediate node records a route to the source node and rebroadcast the RREQ after appending its own address. This is called the path accumulation function. When the destination node receives the RREQ, it responds with RREP to the source node. Each intermediate node that receives the RREP records a route to the destination node. When the source node receives RREP message, the route is established between the source node and the destination node. As path accumulation function can reduce the routing overhead, although the packet size of the routing packet is increased [Dong-Won Kum et al., 2010]. When a link breaks, the source of the packet is notified. RERR message is sent to inform the source node.

3. Wormhole Attack



High speed of channel link
Fig 1. Wormhole attack

Wormhole is a severe type of attack, where two attackers are connected to each other through high speed off-channel link. In this wormhole node receives the packet at one location and send it to other wormhole node through high speed off-channel link. The worst can happen that nodes can be in dilemma that they are close to the destination even though they are at far distance.

Three types of wormhole attack are:
1. All Pass: In this wormhole nodes will pass all the packets irrespective of their size.
2. All Drop: In this all the packets are dropped by wormhole nodes.
3 Threshold: Wormhole drops all the packets size greater than or equal to the threshold value.

4. Simulation And Results

The Qualnet 5.2 simulator is used for simulation. The MAC protocol IEEE 802.11 was used with a data rate of 2 Mbps.

Table 1. Simulation Parameters

Parameter	Value
Terrain Size	1500m×1500 m
No. of Nodes	25/50/75/100
No. of wormhole nodes	4/8/12/16
Traffic Type	CBR
No. of CBR links	5
Mobility Model	Random Waypoint
Routing Protocols	AODV, DYMO
MAC	802.11
Packet Size	512 bytes
Speed	0-10m/s
Pause Time	10 sec
Simulation Time	400 sec
Attack Type	Wormhole

4.1 Performance Metrics

Performane Metrics used to measure the performance are:

4.1.1 Packet Delivery Ratio: Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source.

4.1.2 Average End-to-End Delay: Average end-to-end delay is the average time it takes a data packet to reach to destination in seconds. It is calculated by subtracting “time at which first packet was transmitted by source” from “time at which first data packet arrived to destination.

4.1.3 Throughput: It is defined as total number of delivered data packets divided by the total duration of simulation time.

4.1.4 Jitter: Jitter is the variation in the time between packets arriving, caused by network congestion, and route changes.

Results without wormhole attack

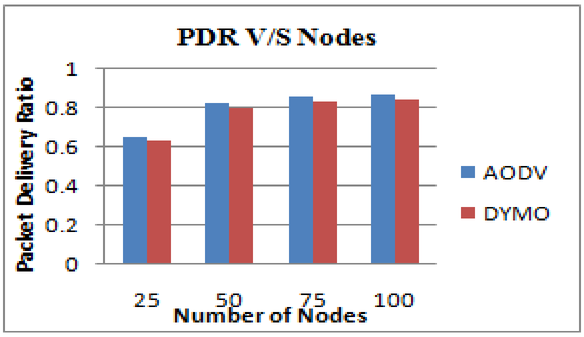


Fig 2: PDR without wormhole

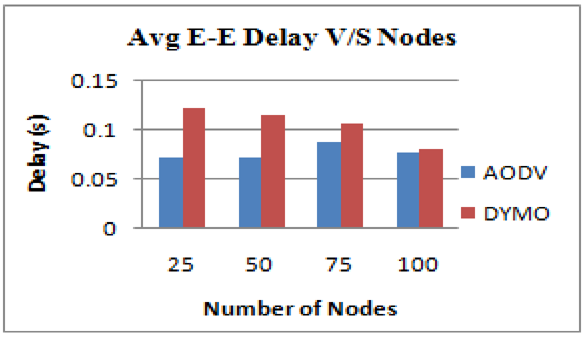


Fig 3 Avg. E-to-E Delay without wormhole

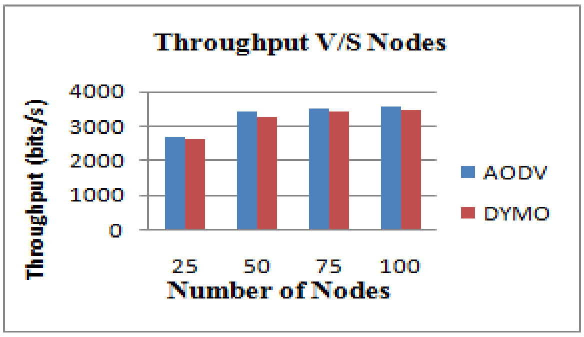


Fig. 4 Throughput without wormhole

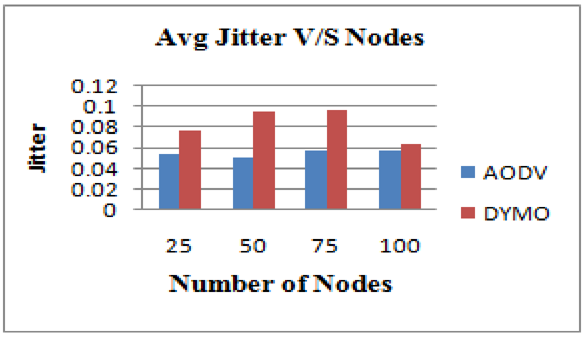


Fig. 5 Avg. jitter without wormhole

Results with Wormhole

- **All Pass**

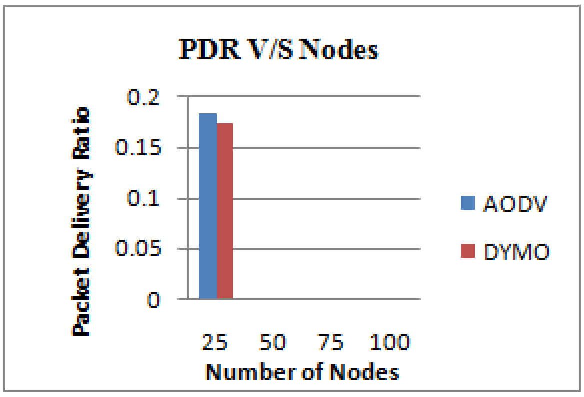


Fig. 6 PDR for All Pass mode

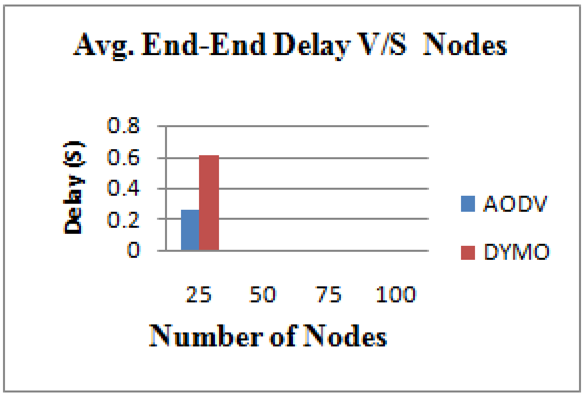


Fig. 7 Avg. E-to-E Delay for All Pass mode

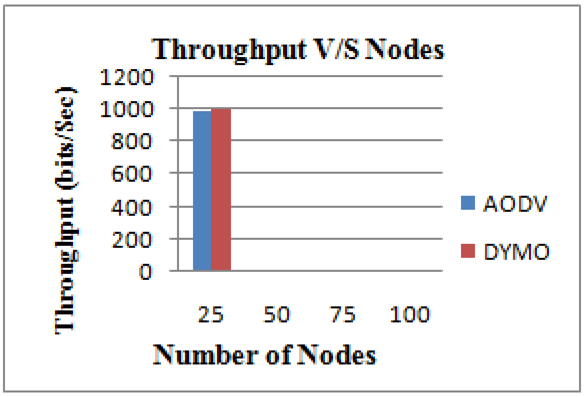


Fig. 8 Throughput for All Pass mode

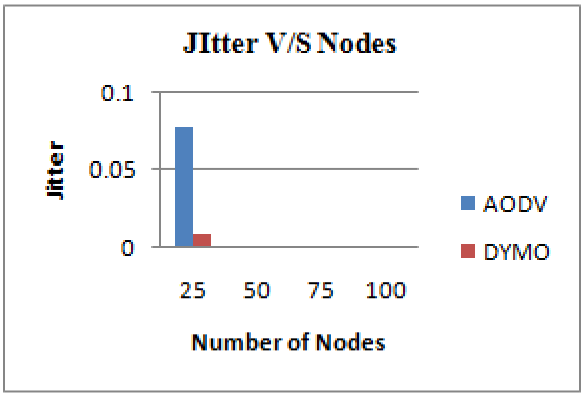


Fig. 9 Avg. Jitter for All Pass mode

- **ALL Drop** In all drop, all the packets that are sent by the sender to the receiver are dropped by the wormhole nodes.

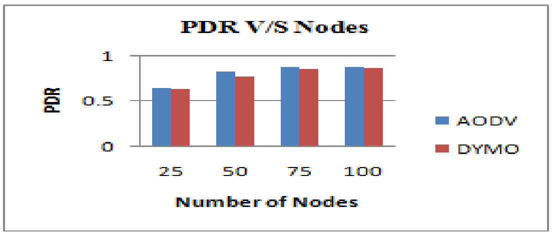


Fig. 10 PDR for All drop mode

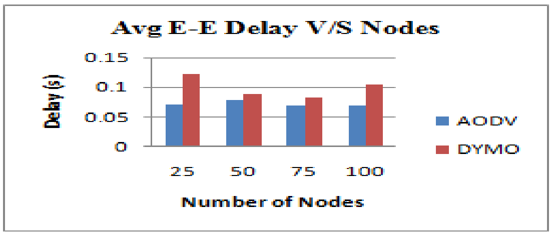
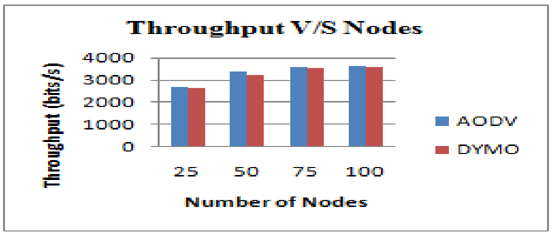


Fig. 11 Avg E-to-E Delay for All Drop mode



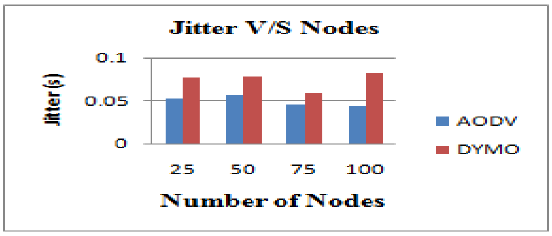


Fig. 12 Throughput for All Drop mode

Fig. 13 Avg Jitter for All Drop mode

- **Threshold (150 Bytes)** In this case, wormhole drops all the packets which are above 150 bytes in size.

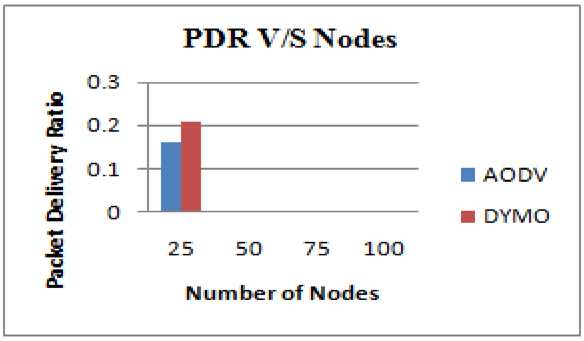


Fig. 14 PDR for Threshold mode

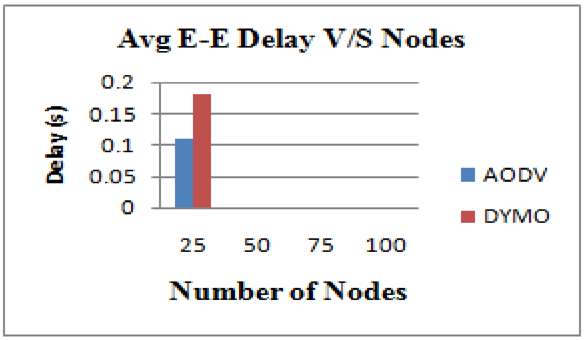


Fig. 15 Avg. E-to-E Delay for Threshold mode

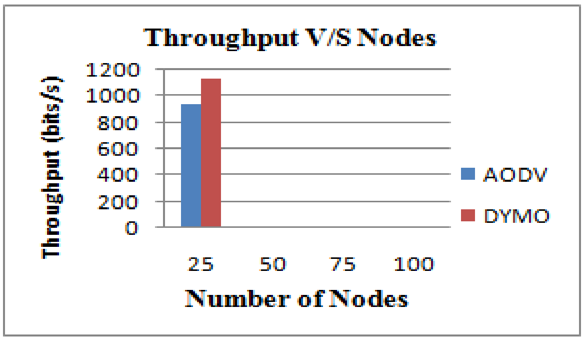


Fig. 16 Throughput for Threshold mode

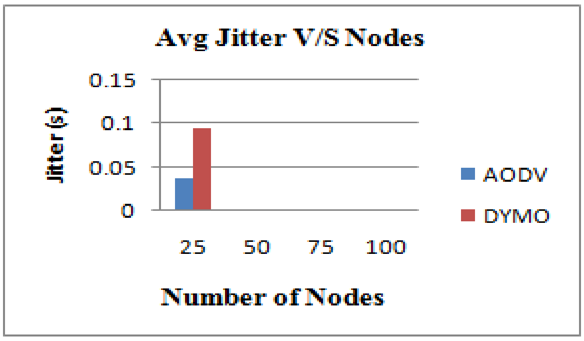


Fig. 17 Jitter for Threshold mode

5. Conlusion And Future Work

From simulation results it is concluded that AODV perform better than DYMO without wormhole attack. But under the wormhole attack the performance of bothe the protocols decreased. But still AODV has better performance than DYMO. All Pass and Threshold has effected the performance greatly. At 25 nodes it has shown some results but as the number of nodes increased the wormhole nodes came into existance and decreased the performance completely. All drop has less affect on the performance as it drop the route request packets and routes are established through other nodes in the network.In future work performance can be measured with different performance metrics like routing overhead by varying pause time and speed. Security mechanism to prevent from these types of attacks can also be developed.

References

[1] Priti Garg, Asma Tuteja. Comparative Performance Analysis of Two Ad-hoc Routing Protocols, International Conference on Network and Electronics Engineering, IPCSIT vol.11,IACSIT Press, Singapore, 2011.

[2] Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade. Mobile Ad Hoc Networking: Imperatives and Challenges, IJCA Special Issue on "Mobile Ad-hoc Networks", 2010.

[3] Jeroen Hoebeke, Ingird Moerman, Bart Dhoebt and Piet Demeester, , An Overview of Mobile Ad-hoc Networking: Applications and Challenges, 2006.

[4] S. Suresh kumar, T. V.P Sundararajan and A Shanmugam. Performance Comparison of three types of wormhole attack in Mobile Adhoc Network, proceedings of the international conference on information science and applications, Chennai, India, 2010.

[5] Gurjinder Kaur, V. K Jain and Yogesh Chaba. Wormhole attacks: Performance Evaluation of On Demand Routing Protocols in Mobile Ad-hoc Networks, world conference on information and communication technologies,pp. 1155-1158, 2011.

[6] Dong-Won Kum, Jin-Su Park, You-Ze Cho and Byoung-Yoon Cheon. Performance Evaluation of AODV and DYMO Routing Protocols in MANET, IEEE CCNC, 2010.

[7] Fahim Maan, Nauman Mazhar. MANET Routing Protocols vs Mobility Models: A Performance Evaluation,ICUFN, 2010.

[8] MIAO Quan-xing, XU Lei. DYMO Routing Protocol Research and Simulation Based on NS2 International Conference on Computer Application and System Modeling, 2010.

[9] Rashid Sheikh, Mahakal Singh Chandel, durgesh Kumar Mishra. Security issues in MANET: A Review, IEEE, 2010.