Performance Comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment

Richa Agrawal
Ph.D. student
ECED, MNNIT Allahabad

Rajeev Tripathi
Professor and Head of the Department
ECED, MNNIT Allahabad

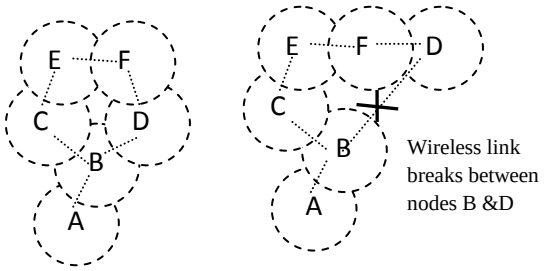
Sudarshan Tiwari
Professor
ECED, MNNIT Allahabad

ABSTRACT
A Mobile Ad-Hoc network, or MANET, is an infrastructure less, self-configuring network. All wireless devices in MANETs are connected through wireless links. Mobile wireless networks are more vulnerable to information and physical security threats than fixed wireless networks. Due to the use of open and shared broadcast wireless channel and due to insufficient physical protection, these networks are prone to security threats. These threats can endanger the overall functionality of mobile ad- hoc network. Various security threats show their impact at different layers. In this paper we have discussed some basic routing protocols. Different security attacks have also been discussed. We consider the wormhole attack as routing attack and based on simulation study we compare the impact of wormhole attack on AODV and DYMO MANET routing protocols.

General Terms
MANET routing protocols, MANET security, Wormhole attack.

Keywords
MANET, AODV, DYMO, DSR, Wormhole.

1. INTRODUCTION
A mobile ad hoc network (MANET) [1] is a group of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes. A simple MANET example is illustrated in Figure 1 [2].



(a) (b)

Fig 1: MANET Topology changes

Dotted circle shows the communication range of particular node and nodes which are in direct communication range of other nodes are connected through wireless links.

Here it is shown, in ad hoc networks due to mobility wireless link breaks that origins changes in the network topology. Initially, the network has the topology shown in Figure 1(a) but when node D moves out of the radio range of node B, the network topology changes to the one in Figure 1(b).
When node D moves out of node B's radio range, link is broken. Nevertheless, the network remains connected since node B can reach node D through nodes C, E, and F.
Since ad hoc networks can be deployed any time anywhere for communication of important informations, so security considerations of these informations are important. Security in mobile ad hoc networks is difficult to achieve, because of vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of centralized monitoring or management point. Security requirements in ad hoc networks are different from those of fixed networks. While the security requirements are the common ones, namely availability, confidentiality, integrity, authentication and non-repudiation, they are considered differently for ad hoc networks due to system constraints in mobile devices (i.e. low power microprocessor, small memory and bandwidth, short battery life) and frequent network topology changes.
Routing in ad hoc networks has become a popular research topic. These MANET routing protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [3][4], nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [5], nodes obtain routes by periodic exchange of topology information. In this article we provide an overview of AODV and DYMO [6] routing protocols.
Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. However, in a hostile environment, a malicious node can launch routing attacks to disrupt routing operations. Recently, several research efforts were launched to counter against these malicious attacks [7].
In this article, we have presented brief overview of security requirement of MANETs and various routing attacks against MANETs at different routing layers. Then, we have discussed wormhole attack [8][9]. The rest of this article is organized as follows:
In section V we have presented some previous work related to wormhole attack. Section VI and VII contains some parameters related to simulation, and the definitions of metrics that we have used for simulation purpose. In section VIII we have shown various graphs of routing protocols simulated on QualNet software [10] and discussed the results obtained from the simulation.
Section IX includes some discussion about the nature of graphs and gives some directions for the improvement of existing protocols. It also shows the strong need of development of security aware routing protocols for successful and secure communications.

2. ROUITNG PROTOCOLS IN MANETs

The aim of a MANET routing protocol is to ascertain the most recent, stable and correct route to a specific destination for a continuously changing network. Routing protocols in a MANET can be classified into two categories: reactive routing protocols (e.g., AODV), in which source initiates route discovery when needed and proactive routing protocols (e.g., OLSR), in which nodes exchange routing table periodically, even there is no active communication between nodes. There are various MANET routing protocols as no single routing protocol work well in all environments. In this section, we describe two reactive routing protocols AODV and DYMO that currently are being researched actively.

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

The Ad Hoc On-Demand Distance Vector Routing Protocol is purely an on-demand routing protocol. Mobile nodes that do not want to take part in active communication need not to maintain any routing table and not to exchange periodical routing informations between nodes. AODV is an improvement of the DSDV algorithm [11]. It utilizes broadcast route discovery mechanism and monotonically increasing destination sequence number to provide most recent route to destination. It provides faster route convergence, low. AODV operation can be understood in two steps: Path Discovery and Path Maintenance [1][4][5]. Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) are the messages types used in AODV routing protocol.

2.1.1 Path Discovery

AODV nodes maintain a route table in which next-hop routing information for destination node is stored. To start path discovery, the source node creates a route request (RREQ) packet. This packet contains the source's IP address, the destination's IP address, source sequence number, the last destination sequence number, packet broadcast number and hop count. Figure 2(a) illustrates this flooding procedure. Source node A wants to communicate with destination node H. After creating the RREQ message, the source broadcasts the RREQ to its neighbors. After releasing every new RREQ packet broadcast number is incremented. When a neighboring node receives a RREQ, it first creates a reverse route to the source node. The node from which it receives the RREQ, the hop count number is increments by one to get the hop distance from the source. In this manner, the RREQ floods the network in search of a route to the destination. After receiving similar copies of the same RREQ packet as forwarded by it before, intermediate nodes drop all the packets.

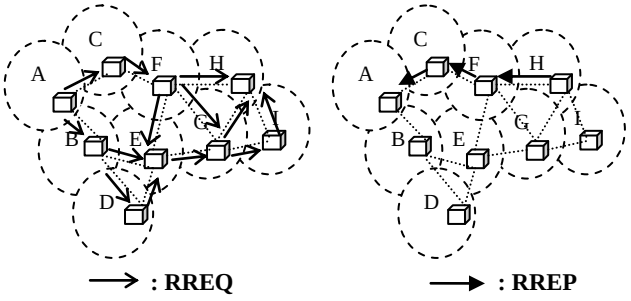


Fig 2(a): RREQ Broadcast **Fig 2(b): RREP Propagation**

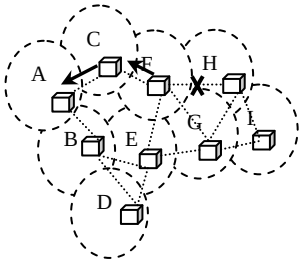


Fig 2(c): RERR Message

Fig 2: AODV route discovery and maintenance

After receiving RREQ packet, destination node H unicasts a RREP packet to the source node A. The reverse route as created above is utilized to send RREP hop by hop back to the source node (Figure 2(b)). Once the source receives the RREP, it can utilize the path for the transmission of data packets.

2.1.2 Path Maintenance

Due to highly dynamic nature of mobile nodes, when a link break along an active route occurs, the node upstream of the break invalidates the routes to each of those destinations in its route table. It then creates a route error (RERR) message and unicast it to the source. As in Figure 2(c), when a link break between nodes F and H occurs, node F immediately unicasts a RRER message back to the source node A, to inform the unavailability of route to the destination node H. Periodical hello messages can be used to detect link breaks. If the current active path has been broken then source restarts path discovery process if it wants to communicate with destination node. Now node increments last known sequence number by one in its RREQ packet and broadcast it to its neighbors for finding fresh enough route.

2.2 Dynamic MANET On-Demand Routing Protocol (DYMO)

DYMO is not a new protocol but an improvement of basic AODV routing protocol and easier to implement. It operates similar to AODV, which we described in section 2.1. It is intended for use by mobile nodes in wireless, multihop networks. DYMO [6][12] determines unicast between DYMO routers within the network in an on-demand fashion, offering improved convergence in dynamic topologies. The basic operations of the DYMO protocol are route discovery (by route request and route reply) and route maintenance. In networks with a large number of routers, it is best suited for sparse traffic scenarios. In each DYMO router, minimal state routing is maintained and therefore it is applicable to memory constrained devices. In this protocol only routing information relative to active sources and destinations is maintained. The routing algorithm in DYMO may be operated at layers other than the network layer, using layer-appropriate addresses. For operation at other layers only modification of the packet/message format is required. To ensure predictable control overhead, DYMO router's rate of packet/message generation should be limited. The protocol is suitable for

scalability. However, it is yet to be explored for its functionality.

2.2.1 Route Discovery

A source node issues a RREQ if it wants a route to any particular destination. Each intermediate node that receives the route request packet records the route to the source node. When the destination node receives the RREQ it unicasts a RREP packet to the source node. Each intermediate node that receives the RREP packet records a route to the target node. After sending a RREQ, source node wait up to RREQ_WAIT_TIME for route creation and send another RREQ if it does not receive any RREP message. To avoid excessive overheads in route discovery process source uses binary exponential back off. Next time it generates a RREQ, it waits for twice of the previous wait time. This process continues up to a total RREQ_TRIES. Waiting data packets remain in buffer and dropped if route to the desired destination is not obtained within the maximum number of RREQ_TRIES [6].

2.2.2 Route Maintenance

Due to dynamic nature of MANET, frequent link breaks occur, which results in change in network topology. Route maintenance consists of two phases. First it is checked that route that are used for forwarding the packet is valid or not. If the route life time has been expired the packet cannot be forwarded and RERR message is generated. In the second phase, when the route towards a certain destination is unknown, RERR messages are generated for notification of the involved nodes. Upon receiving a RERR, a node deletes the specified route.

3. SECURITY REQUIREMENTS

Security in a MANET is an essential component for basic network functions like packet forwarding and routing [8] [13]. Following are some basic requirements that effective security architecture must ensure in order to combat passive and active attacks.

- **Availability**: ensures that services offered by the node will be available all the time to its user when expected.
- **Authorization:** nodes must be able to authenticate that the data has been sent by the legitimate node.
- **Confidentiality:** ensures that a given message could be understood only by intended receivers.
- **Integrity:** ensures that message has been transmitted to intended receiver with any alteration of original message.
- **Non-repudiation:** means that sender cannot deny after sending any message and also receiver cannot deny after receiving of any message.

4. SECURITY THREATS

Any action that can affect the security in the ad hoc network is known as security threats that can be divided as [7][16].

4.1 Attacks

- ***External attacks:*** Nodes that are not part of network or they do not have authority to access the network can launch external attacks.
- ***Internal attacks:*** Nodes that are active part of the network can launch internal attacks.
- ***Active attacks:*** These types of attacks can be launched by any node in the network, actively interacting with legitimate nodes in the network.
- ***Passive attacks:*** A passive attacker eavesdrops the packets from the network, analyzes them and collects the required information to launch an active attack later.

4.2 Misbehavior

The aim of the node's misbehavior in the network is not to launch an attack in the network, but to obtain an unfair advantage such as saving its resources, compared with the other nodes in the network.

These security threats affect the functioning of the network at different OSI layers. The physical layer is the first layer of the OSI reference model. The main threats at physical layer are passive eavesdropping, signal jamming and interference. At link layer attackers may launch Denial of Service attack at which an attacker may send large number of routing traffic in the network for consuming useful network resources [2][14]. Several attacks which affect the functioning of network layer are blackhole attack, wormhole attack, rushing attack, byzantine attack etc. Some attacks at transport layer are SYN flooding, session hijacking and TCP ACK storm. Serious attack at application layer is repudiation attack [8][15][16].
This paper focuses on the wormhole attack, where two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. Then we have compared the impact of wormhole attack on AODV and DYMO manet routing protocols.

4.3 Wormhole Attack

Mobile ad hoc networks are more susceptible to to security attacks than other wireless networks due to absence of any fixed security service provider. Each node in the network may not be a legitimate node, some of them may work maliciously. There are various security attacks which can harm even destroy the whole functionality of the network.

Wormhole attackers affect seriously the original functionality of MANET routing protocols. Two malicious nodes in the network compromise with each other and form a high speed directional link for the network traffic. They accept the traffic at one location of the network, tunnel them through directional link and replay packets into the other locations of the network. If the link formed by colluding nodes is longer than normal wireless link of single hop, the packets reach sooner to the destination using wormhole link than ordinary wireless links.

If RREQ packets pass through wormhole channel and wormhole attacker do not alter any field of RREQ packets, they simply tunnel the packets to the other end then it will be useful as the packet reaches the destination sooner. Wormhole attackers generally alter data fields of RREQ packets and convey wrong information to the network nodes by relaying altered packets.

The wormhole places the attackers in a powerful position relative to other nodes, so that it may attract maximum traffic towards itself for destroying the network functionality.

For example in Figure 3[8], for a reactive routing protocol, source node S want to communicate with the destination node D. Nodes M1 and M2 are malicious nodes (wormhole attackers) and form a high speed wireless link M1M2. Nodes L1, L2, L3, L4, L5, L6, L7and L8 are the legitimate nodes of the network. When node S starts route discovery it sends

RREQ packet to the neighboring nodes. L1and L4 are neighboring nodes, they are not destinations so they forward RREQ packet to their neighbors. Now nodes M1 and L5 both receive the RREQ packet, but node M1 forms wormhole link with node M2 and forwards RREQ packets faster than node L5. thus the path from source to destination includes wormhole link. Thus all the traffic reaches to the destination by passing through Wormhole tunnel.

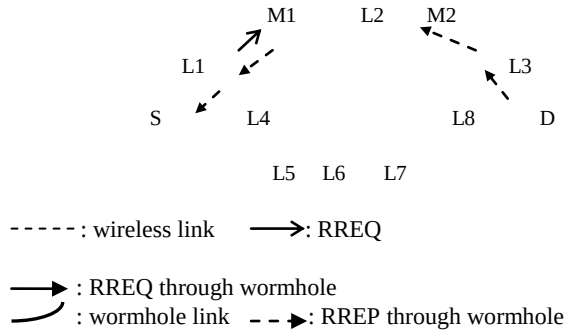


Fig 3: An example of wormhole attack

5. RELATED WORK

This paper focuses on the wormhole attack, where two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. This lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel.

In [17], a particular type of wormhole attack known as "in-band wormhole attack" is identified. A game theoretic approach has been followed to detect intrusion in the network. Presence of a central authority is assumed for monitoring the network. This is a limitation in wireless scenario, such as military or emergency rescue. No experimental result is reported in [17].

In [18], the wormhole attacks are classified as:

1) In-band wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole attack, which require a hardware channel to connect two colluding nodes. The in-band wormhole attacks are further divided in :

- Self-sufficient wormhole attack, the attack is limited to the colluding nodes and
- Extended wormhole attack, the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them.

6. SIMULATION WORK

The simulations were performed using QualNet simulator version 5 [10]. In this scenario the source-destination pairs are spread randomly over the network. The model parameters that have been used in he following experiments are summarized in Table1.

Table 1. Parameters for simulation

Parameters	Values
Topographical area	1500*1500 sq.m.
Channel type	Wireless channel
Radio-propagation model	TwoRayGround
Antenna type	Omni antenna
Interface queue type	Drop Tail/PriQueue
MAC type	802.11, Worrmhole
Routing protocols	AODV, DYMO
Node density	20, 40, 60, 80,100/1500*1500 sq.m.
Mobility model	Random waypoint
Mobility scenario	10m/s to 50m/s
Application traffic	CBR
CBR packet size	512 bytes

We have tested the performance metrics of two routing protocols (AODV & DYMO) with and without wormhole attack scenario. Also different wormhole metrics for two routing protocols are compared. The varying parameters are mobility speed (10-50m/s), no. of nodes (20-100) & simulation time (100-500sec).

7. PERFORMANCE METRICS CONSIDERED FOR EVALUATION

- **Throughput:** Throughput of any network scenario is defined as no. of information packets or bits delivered per second to the destination.
- **Packet loss:** Packet loss is defined as no. of packets that are generated at source node but cannot be successfully delivered to the destination node within valid time.
- **Average end-to-end delay:** Average end-to-end delay of the data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.
- ***Wormhole parameters:***
  - **Frames intercepted all:** Number of frames intercepted by the wormhole node.
  - **Frames dropped by wormhole:** Number of frames dropped by the wormhole link.
  - **Frames tunneled:** Number of frames tunneled by the wormhole node (frames intercepted multiple times due to repetitive replay will not be tunneled).
  - **Frames replayed:** Number of frames replayed by the wormhole node.
  - **Frames dropped by queue:** Number of frames dropped by the queue in the wormhole node

8. RESULT AND ANALYSIS

8.1 Packet loss

The following Figures 4(a), 4(b) and 4(c) shows packet loss for AODV and DYMO routing protocols with and without wormhole attack. As shown in all the graphs, packet loss for AODV protocol is the highest under wormhole attack situation. As DYMO routing protocol is an improved version of AODV protocol, the packet loss is lower for DYMO than AODV.

- Packet loss decreases with the increased movement of nodes because with more speed, probability of intercommunication between nodes increases.
- There is not much change in packet loss with the increase in simulation time.

- Packet loss for all the routing protocols decreases as no. of nodes increases. For very large no. of nodes there is no packet loss because connection establishment probability increases very much with large hosts in the network.
- Packet loss increases with wormhole environment because information packets dropped by malicious nodes forming low latency higher bandwidth link.

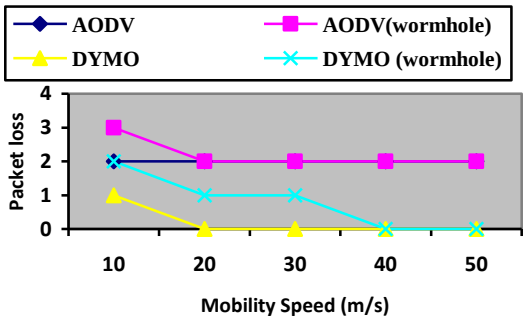


Fig 4(a): Packet loss Vs mobility

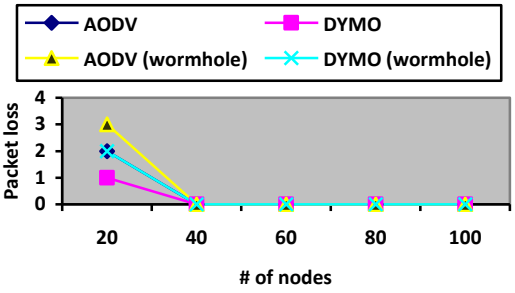


Fig 4(b): Packet loss Vs number of nodes

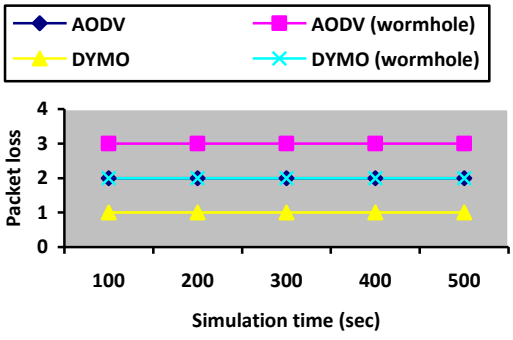


Fig 4(c): Packet loss Vs simulation time

8.2 Average end-to-end delay

As shown in figures 5(a), 5(b) and 5(c), the average end-to-end delay for both the routing protocols under wormhole attack is lower than the delay without wormhole attack because

- A wormhole attacker tunnels messages received in one location in the network over a low-latency high bandwidth link and replays them in a different location.
- Adversaries can forward packets faster than regular nodes that require a queuing delay, transmission delay, and MAC contention delay. Hence average end-to-end delay for packets under wormhole environment is less than without wormhole environment.
- Average end-to-end delay decreases with increase in mobility and no. of nodes as both probability of communication and probability of path establishment between different nodes increases.
- There is not much change in average delay with variation time because it is not necessary that a better link could be established between communicating nodes during simulation time.

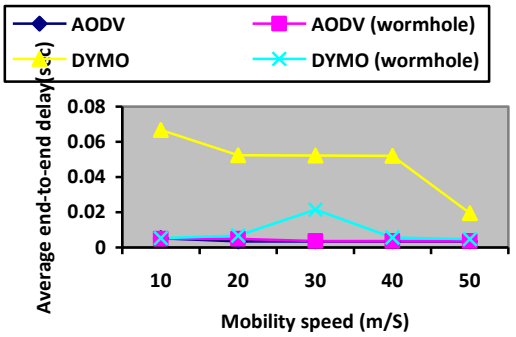


Fig 5(a): Average end-to-end delay Vs mobility speed

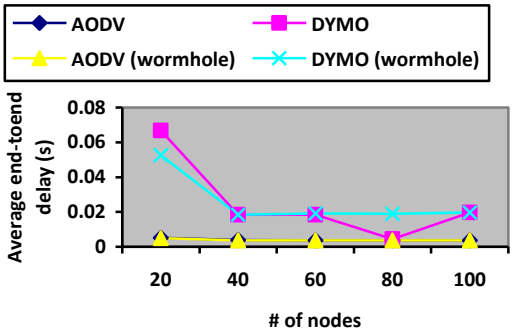


Fig 5(b): Average end-to-end delay Vs number of nodes

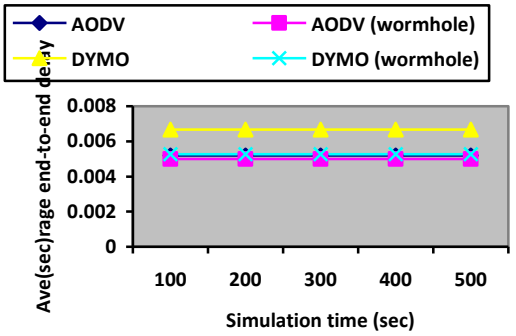


Fig 5(c): Average end-to-end delay Vs simulation time

8.3 Throughput

As shown in Figures 6(a), 6(b) and 6(c), throughput for DYMO routing protocol is higher as compared to AODV

routing protocol. Also throughput under wormhole attack environment is always lower than the throughput without attacking environment, because under wormhole attack environment information packets are dropped by malicious nodes. Once the attacking nodes know they are en route, they can launch a black hole attack to drop all data packets, or a grayhole attack to selectively drop some critical packets.

- As mobility increases, throughput for routing protocols also increases but with the wormhole attack there is no change in throughput with mobility, because once attacker form a wormhole colluding link, they continuously drop data packets routed towards destination.
- With increase in no. of nodes AODV do no show any significant variation but with increase in no. of nodes throughput of DYMO routing protocol increases for both attack and without attack environment.
- There is not much effect of simulation time on the throughput of AODV and DYMO routing protocols.

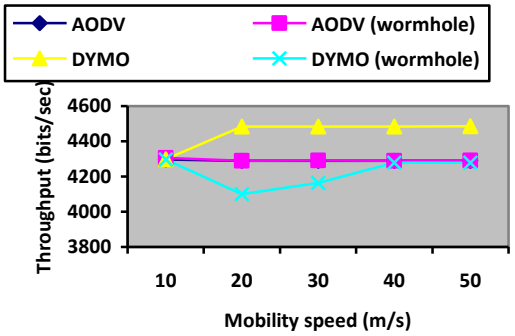


Fig 6(a): Throughput Vs Mobility speed

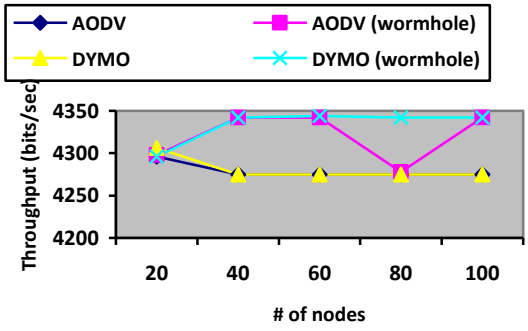


Fig 6(b): Throughput Vs number of nodes

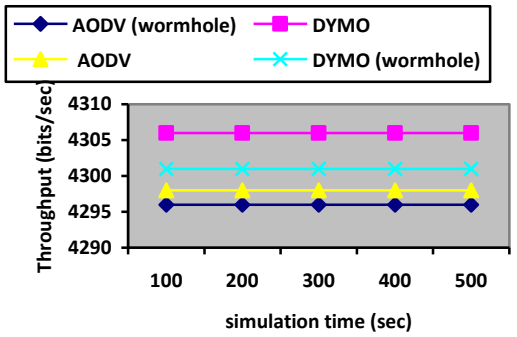


Fig 6(c): Throughput Vs simulation time

8.4 Wormhole parameters

As shown in figures 7(a), 7 (b) and 7(c), the effect of wormhole attack on DYMO protocol is more than AODV protocol.

- With increasing simulaton time, all the womhole parameters increases.
- As No. of nodes in the network inceases, no. of frames interceped, tunneled, dropped by wormhole and replayed also increases.
- With inceasing mobility the wormhole parameters increases, but at higher mobility there is not very much variation in wormhole parameters. The no. of replayed packets are in very small numbers for AODV routing protocol.

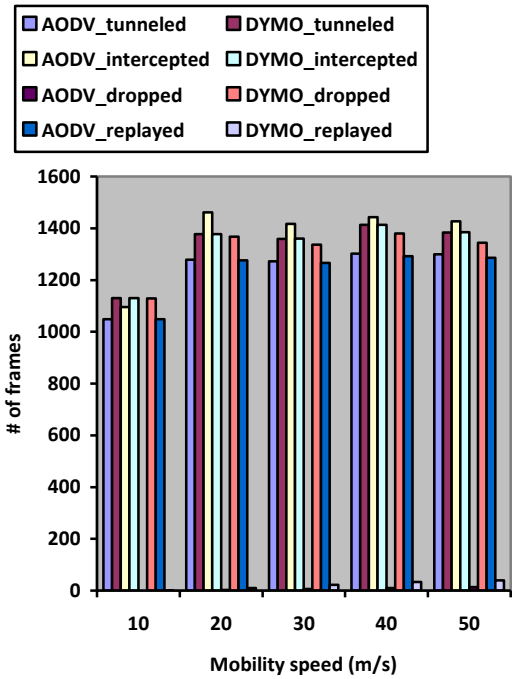


Fig7(a): Wormhole parameters Vs mobility speed

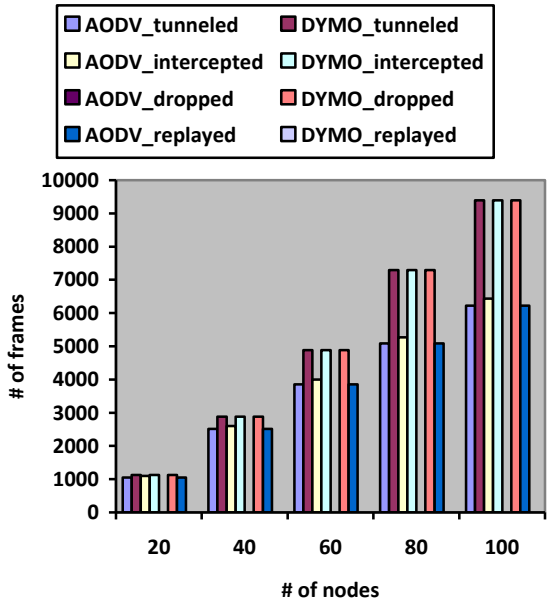


Fig 7(b): Wormhole parameters Vs number of nodes

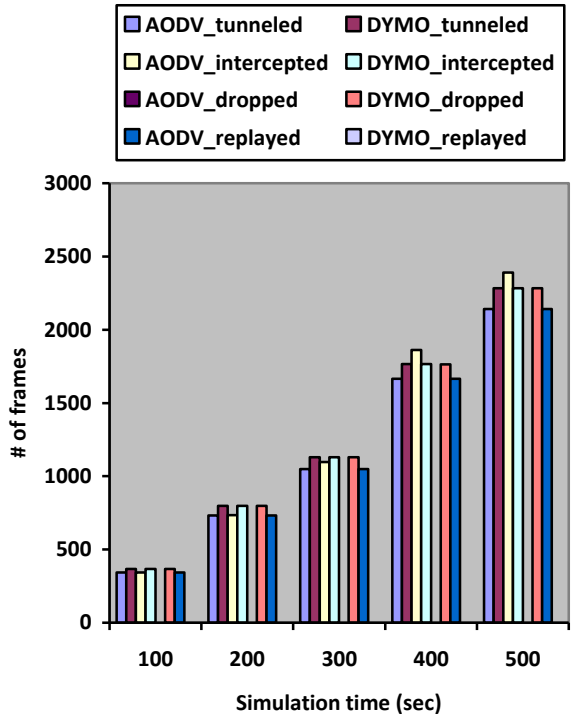


Fig 7(c): Wormhole parameters Vs simulation time

9. CONCLUSIONS AND FUTURE WORK

We have evaluated two reactive routing protocols AODV and DYMO varying various network parameters and compared their performances with and without wormhole attack environment. After examining the graphs given in section 8 carefully, it is clear that AODV routing protocol was more affected than DYMO protocol by mobility, simulation duration and network density. Due to its routing mechanism the behavior of AODV is better than DYMO.

Future work may include further investigation of routing message processing mechanism of AODV to improve its performance and also try to develop scalability and mobility aware extensions of AODV protocol.

Performance of both the protocols degrades under wormhole attack environment. So the presence of such type of attacker is very dangerous as the whole purpose of our communication system may be destroyed. Therefore trustworthy techniques that may detect and prevent the wormhole attack should be used. Also there may be many other serious threats for network. So their prevention scheme should also be discovered. There is very much need to focus over developing such type of routing mechanism which may work under varying manet environment and can protect different severe security threats.

10. ACKNOWLEDGMENTS

My sincere thanks to my honourable guides Prof. Sudarshan Tiwari and Prof. Rajeev Tripathi who have motivated me strongly and contributed towards the preparation of the paper.
I am also thankful to my family membrs and friends for their all-time support.

11. REFERENCES

[1] Basangi, S., Conti, M., Giordano, S. and Stojmenovic, I. 2004. Mobile ad hoc networking. IEEE Press. Wiley-Interscience. P-282.

[2] Komninos, N., Vergados, D. and Dougligeris, C. 2006. Layered Security Design for mobile ad hoc networks. Computers & Security. Elsevier.

[3] Perkins, C. E., Royer, E.M. 1999. Ad-hoc on-demand distance vector routing. Mobile Computing Systems and Applications. Proceedings. pp. 90–100.

[4] Perkins, C. E., Royer, M., and Das, S. 2003. Ad-hoc on-demand distance vector routing. IETF. RFC 3561.

[5] Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A. and Viennot, L. 2003. The optimised routing protocol for mobile ad-hoc networks: protocol specification. Hipercom, INRIA. October.

[6] Chakeres, I. D. and Perkins, C. E. 2006. Dynamic MANET on-demand (DYMO) routing protocol. IETF. Internet-Draft Version 6. October.

[7] DjeNouri, D. and Khelladi, L. 2005. A survey of security issues in mobile ad hoc and sensor networks. IEEE Communication Surveys and Tutorials. Fourth Quarter. Volume 7, No. 4.

[8] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. and Jamalipour, A. 2007. A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications. October.

[9] Hu, Y-C. Perrig, A. and Johnson, D. 2006. Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications. Volume 24. No. 2. February.

[10] Scalable Network Technologies. QualNet simulator-version 5.02. Software package. Available online: http://www.qualnet.com.

[11] Perkins, C. E. and Bhagwat, P. 1994. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. Published by ACM 1994 Article.

[12] Espensen, K. L., Kjeldsen, M. K. and Kristensen, L. M. 2007. Towards modelling and validation of the dymo routing protocol for mobile ad-hoc networks. Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools. Eighth Workshop. Aarhus, Denmark, October 22-24.

[13] Argyrouds, P. G. and O'Mahony, D. 2005. Secure routing for mobile ad hoc networks. IEEE Communications, Third Quarter, Volume 7, No. 3.

[14] Khan, S., Mast, N. Loo, K-K. 2009. Denial of service attacks and mitigating techniques in IEEE 802.11 Wireless Mesh networks. Information: An International Interdisciplinary Journal. Volume 12. No. 1. January.

[15] Hu, Y., Perrig, A. and Johonson, D. B. 2003. Rushing attacks and defence in wireless ad hoc network routing protocols. Proceedings ACM Workshop. Wireless Security. September pp. 30–40.

[16] Buchegger, S. and Boudec, J. Y. 2002. Nodes bearing grudges: toward routing security, fairness and robustness in mobile ad hoc networks. 10th Euromicro Workshop. Parallel, Distributed and Network-based Proceedings.

[17] Baras, J. S., Radosavac,S. and Theodorakopoulos, G. 2007. Intrusion detection system resiliency to byzantine attacks: the case study of wormholes in olsr. Military Communications Conference (MILCOM). Orlando, Florida.

[18] Mahajan, V., Natu, M., and Sethi, A. 2008. Analysis of wormhole intrusion attacks in MANETS. Military Communications Conference. San Diego. IEEE, pp.1-7 .