# A Behavioral Study of Wormhole Attack in Routing for MANET

Amrit Suman
CSE Department.
Technocrats Institute of Technology, Bhopal

Praneet Saurabh
CSE Department.
Technocrats Institute of Technology, Bhopal

Bhupendra Verma
CSE Department.
Technocrats Institute of Technology, Bhopal

## ABSTRACT
Wireless mobile ad-hoc networks are those networks which has no physical links between the nodes. There is no fixed topology in this network due to the random mobility of nodes, interference, multipath propagation and path loss. Many Routing protocols have been proposed and developed for accomplishing this task. The intent of this paper is to analyze three ad-hoc routing protocols AODV, DYMO, FISHEYE against wormhole attack in wireless network. This paper concentrates evaluating the performance of routing protocols when wormhole attacks involve in wireless network. The performance analysis for above protocol is based on variation in speed of nodes in a network with 50 nodes. All simulation is carried out with QualNet 5.0 simulator.

## Keywords
Ad Hoc Networks, routing protocol, Wormhole attack, AODV, DYMO, FISHEYE.

## 1. INTRODUCTION
Mobile ad hoc networks (MANETs) [1,2] are collections of mobile nodes, which are Dynamically form a temporary network without pre-existing network infrastructure or any centralized administration. These nodes can be arbitrarily located and are free to move randomly at any given time. Every mobile node acts itself as a router. Since there is no centralized administration, so MANET is oftenly called autonomous. MANET implies that the topology may be dynamic - and that routing of traffic through a multi-hop path is necessary if all nodes are to be able to communicate. A key issue in MANETs is the necessity that the routing protocols must be able to respond rapidly to topological changes in the network. At the same time due to the limited bandwidth available through mobile radio interfaces it is imperative that the amount of control traffic generated by the routing protocols is kept at a minimum. Several protocols have been addressed these problems of routing in mobile ad-hoc networks. These protocols were divided into two classes: depending upon the type of requirement and the available resources, when a node acquires a route to a destination.

***Proactive*** protocols [3, 4] are characterized by all nodes maintaining routes to all destinations in the network at all times. Thus using a proactive protocol a node is immediately able to route (or drop) a packet. Examples of proactive protocols include the "FISHEYE routing protocol". [5], the "Optimized Link State Routing Protocol" (OLSR) [6] and the "Source Tree Adaptive Routing" (STAR) [7]. *Hybrid* protocols [3, 8] are those protocols which have characteristics of both reactive and proactive. Example of hybrid protocol includes "Dynamic MANET On-demand routing protocol" (DYMO) [9]. ***Reactive*** protocols [3] are characterized as the nodes acquiring and maintaining routes ON-demand. In general, when a route to an unknown destination is required by a node, a query is region extraction model provides the much better result any animated scene from natural images. Flooded onto the network and replies, containing possible routes to the destination, are returned. Examples of reactive protocols include the "Ad Hoc on Demand Distance Vector Routing Protocol" (AODV) [9, 13] and "Dynamic Source Routing" (DSR) [10, 14].

In this paper, the analysis of three routing protocols (AODV, DYMO, and FISHEYE) are presented against wormhole attack. The performance of these protocols is analyzed with varying speed of nodes in network. The network contains 50 wireless nodes in which 10 nodes are in wormhole attack. These nodes either stop packet forwarding or send wrong and unusual information to other nodes which affects packet drop and lesser throughput.

In this paper Section 2 briefly describes the routing protocols AODV, DYMO, FISHEYE. Section 3 briefly describes the affects of wormhole attack in network. Section 4 presents experimental configuration. Section 5 focused on results and analysis of the work and Section 6 contains the conclusion.

## 2. ROUTING PROTOCOL
The nature of mobile ad hoc networks makes simulation modeling an invaluable tool for understanding the operation of these networks. In Ad-hoc network multiple routing protocols have been developed during the last years, to find optimized routes from a source to some destination. To establish a data transmission between two nodes, typically multiple hops are required due to the limited transmission range. Mobility of the different nodes makes the situation even more complicated.

The protocols to be used in the Ad Hoc networks should have the following features:

- The protocol should adapt quickly to topology changes.
- The protocol should provide Loop free routing.
- The protocol should provide multiple routes from the source to destination and this will solve the problems of congestion to some extent.
- The protocol should have minimal control message overhead due to exchange of Routing information when topology changes occurs.
- The protocol should allow for quick establishment of routes so that they can be used before they become invalid.

## 2.1. Ad hoc On-Demand Distance Vector (AODV):

The Ad hoc On-Demand Distance Vector (AODV) [8, 12] routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and unicast route determination to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

The primary objectives of AODV protocol are:-

- To broadcast discovery packets only when necessary,
- To distinguishes between local connectivity management (neighborhood detection) and general topology maintenance and
- To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information. AODV decreases the control overhead by minimizing the number of broadcasts using a pure on-demand route acquisition method. AODV uses only symmetric links between neighboring nodes.

## 2.2. Dynamic MANET On-demand routing protocol (DYMO)

The DYMO routing protocol is successor to the popular Ad hoc On-Demand Distance Vector (AODV) routing protocol and shares many of its benefits. It is, however, slightly easier to implement and designed with future enhancements in mind. DYMO [5] can work as both a proactive and as a reactive routing protocol, i.e. routes can be discovered just when they are needed.

In any way, to discover new routes the following two steps take place:

- A special "Route Request" (RREQ) messages is broadcast through the MANET. Each RREQ keeps an ordered list of all nodes it passed through, so every host receiving an RREQ message can immediately record a route back to the origin of this message.
- When an RREQ message arrives at its destination, a "Routing Reply" (RREP) message will immediately get passed back to the origin, indicating that a route to the destination was found. On its way back to the source, an RREP message can simply back trace the way the RREQ message took and simultaneously allow all hosts it passes to record a complementary route back to where it came from.

## 2.3. FISHEYE:

Fisheye [5] Routing determines routing decisions using a table-driven routing mechanism similar to link state. The table-driven ad hoc routing approach uses a connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired. It relies on an underlying routing table update mechanism that involves the constant propagation of routing information. A table-driven mechanism was selected over an on-demand mechanism based on the following properties:

- On-Demand routing protocols on the average create longer routes than table driven routing protocols.
- On-Demand routing protocols are more sensitive to traffic load than Table-Driven in that routing overhead traffic and latency increase as data traffic source/destination pairs increase.
- On-Demand Routing incurs higher average packet delay than Table Driving routing which results from latency caused by route discovery from new destinations and less optimal routes.
- Table-Driven routing accuracy is less sensitive to topology changes. Since every node has a 'view' of the entire network, routes are less disrupted when there is link breakage (route reconstruction can be resolved locally).
- Table-Driven protocols are easier to debug and to account for routes since the entire network topology and route tables are stored at each node, whereas On-Demand routing only contain routes that are source initiated and these routes are difficult to track over time.

For these reasons, a table driven scheme for the ad hoc routing protocol was chosen. Link state was chosen over distance vector because of faster speed of convergence and shorter-lived routing loops. Link state topology information is disseminated in special link-state packets here each node receives a global view of the network rather than the view seen by each node's neighbor. Fisheye routing takes advantage of this feature by implementing a novel updating mechanism to reduce control overhead traffic.

### *2.3.1 Algorithm for FISHEYE routing:*

There are 3 main tasks in the routing protocol:

**1) Neighbor Discovery**: responsible for establishing and maintaining neighbor relationships.

**2) Information Dissemination**: responsible for disseminating Link State Packets (LSP), which contains neighbor link information, to other nodes in the network.

**3) Route Computation**: responsible for computing routes to each destination using the information of the LSPs. Each node initially starts with an empty neighbor list and an empty topology table. After its local variables are initialized, it invokes the *Neighbor Discovery* mechanism to acquire neighbors and maintain current neighbor relationships. LSPs in the network are distributed using the *Information Dissemination* mechanism. Each node has a database consisting of the collection of LSPs originated by each node in the network. From this database, the node uses the *Route Computation* mechanism to yield a routing table for the protocol.

## 3. WORMHOLE ATTACK

An attacker receives packets at one point in the network, "tunnels" them to a different point in the network and then replays them from this point. Tunnel packets received in one place of the network and replay them in another place the attacker can have no key material. All it requires is two transceivers and one high quality out-of-band channel. Most packets will be routed to the wormhole [17]. The wormhole can drop packets or more subtly, selectively forward packets to avoid detection.

## 4. EXPERIMENTAL CONFIGURATION

All the simulation work is performed in QualNet wireless network simulator version 5.0 [3]. Initially number of nodes are 50, simulation time was taken 180 seconds and seed as 1.Seed is a template in QualNet 5.0, in which nodes are placed in network. There are different templates are available in QualNet simulator with different seed number. All the scenarios have been designed with a terrain 1500m x 1500m. Mobility model used is Random Way Point [11] (RWP). In this model a mobile node is initially placed in a random location in the simulation area. For simulation, speed of node is varying from 10mps to 50mps. All the simulation works were carried out using three routing protocols (DSR, ZRP, and STAR) with varying speed of node. Network traffic load is provided by constant bit rate (CBR) application. A CBR traffic source provides a constant stream of packets throughout the whole simulation, thus further stressing the routing task. There are four measurements in our experiments were defined as follows:

1) *Throughput (bits/s):-* Throughput [11, 15] is the measure of the number of packets successfully transmitted to their final destination per unit time.

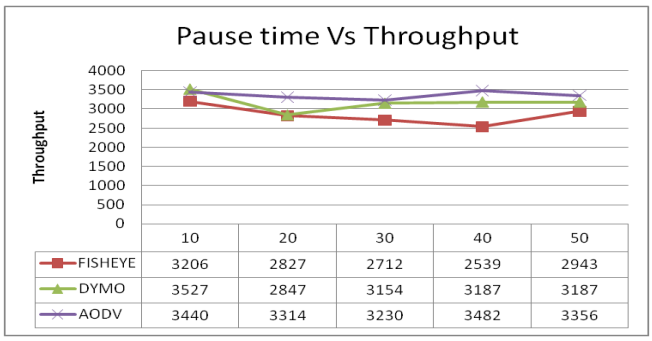
2) *Total Packets received:* - Packet delivery ratio [9] is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).

*3) End-to-end delay*: Average End to End Delay [9, 16] signifies the average time taken by packets to reach one end to another end (Source to Destination)**.**

*4) Average Jitter Effect**:*** Signifies the Packets from the source will reach the destination with different delays [10]. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

## 5. SIMULATION RESULTS & ANALYSIS

**[a]** It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations. It is the ratio between the numbers of sent packets vs. received packets.

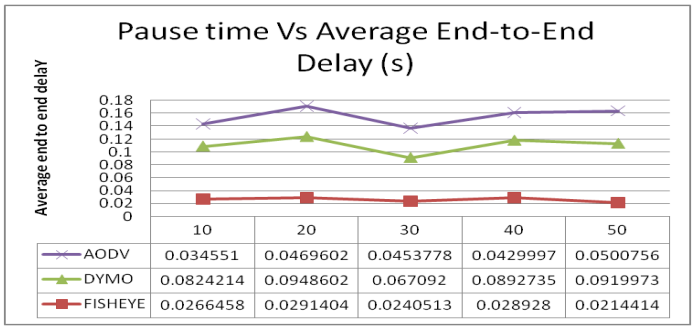



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 3206 | 2827 | 2712 | 2539 | 2943 |
| DYMO | 3527 | 2847 | 3154 | 3187 | 3187 |
| AODV | 3440 | 3314 | 3230 | 3482 | 3356 |

**Figure1**:- Pause Time Vs Throughput

The above figure shows throughput of protocols when pause time varies. It can be observed by throughput of AODV is better than the DYMO and FISHEYE when pause time is kept 10, 20, 30, 40 and 50.

**[b]** Average End to End Delay signifies the average time taken by packets to reach one end to another end (Source to Destination).

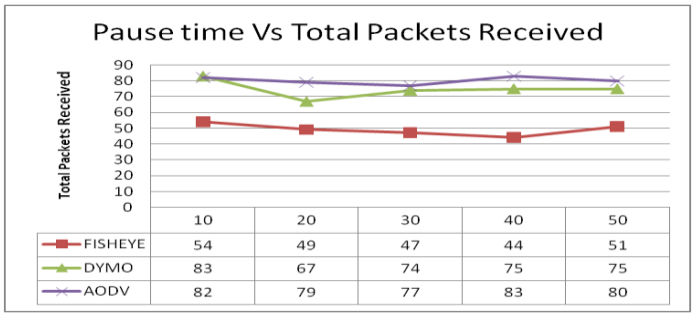



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| AODV | 0.034551 | 0.0469602 | 0.0453778 | 0.0429997 | 0.0500756 |
| DYMO | 0.0824214 | 0.0948602 | 0.067092 | 0.0892735 | 0.0919973 |
| FISHEYE | 0.0266458 | 0.0291404 | 0.0240513 | 0.028928 | 0.0214414 |

**Figure2**:- Pause Time Vs Average End-to-End delay

Figure 2 shows End to End delay of protocols when pause time varieses. It can be observed that End to End delay of FISHEYE is less than other than two protocols, when pause time is kept 10, 20, 30, 40 and 50

**[c]** Total packets received are no. of packets received when sent from source to destination

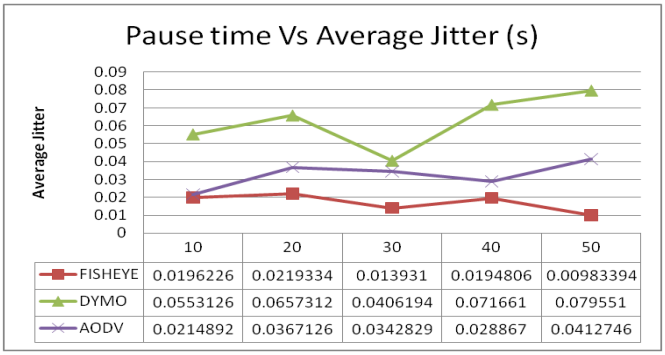



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 54 | 49 | 47 | 44 | 51 |
| DYMO | 83 | 67 | 74 | 75 | 75 |
| AODV | 82 | 79 | 77 | 83 | 80 |

**Figure3**:- Pause Time Vs Total Packets Received

Figure 3 shows Total Packets Received of protocols when pause time varies. It can be observed that total packets received by AODV are greater than other two protocols, when pause time is kept 10, 20, 30, 40 and 50.

**[d]** Average Jitter effect signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

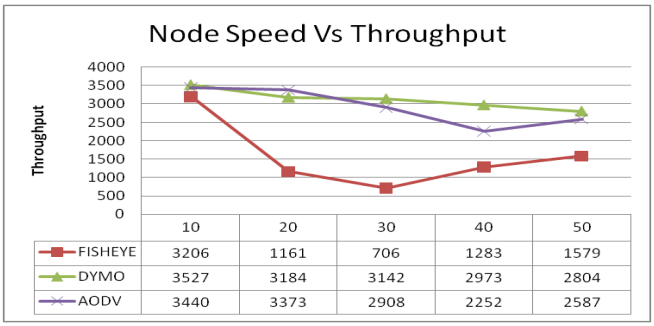



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 0.0196226 | 0.0219334 | 0.013931 | 0.0194806 | 0.00983394 |
| DYMO | 0.0553126 | 0.0657312 | 0.0406194 | 0.071661 | 0.079551 |
| AODV | 0.0214892 | 0.0367126 | 0.0342829 | 0.028867 | 0.0412746 |

**Figure4:-** Pause Time Vs Average Jitter

Figure 4 shows average jitter of protocols when pause time varies. It is observed that average jitter of FISHEYE is less than both AODV, DYMO, when pause time is kept 10, 20, 30, 40 and 50.

**[e]** Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets.

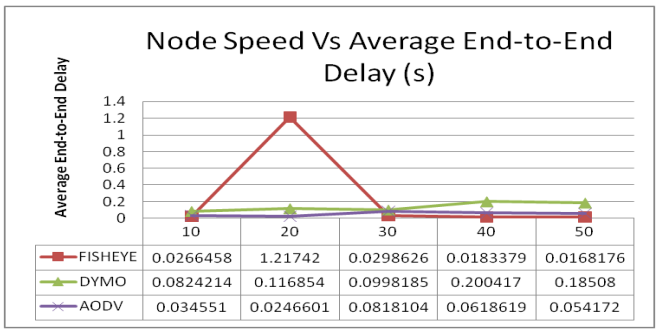



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 3206 | 1161 | 706 | 1283 | 1579 |
| DYMO | 3527 | 3184 | 3142 | 2973 | 2804 |
| AODV | 3440 | 3373 | 2908 | 2252 | 2587 |

**Figure5**:- Node Speed Vs Throughput

Figure 5 shows throughput of protocols when node speeds in network varies. It is observed that throughput AODV is better than FISHEYE and DYMO, when speed of node in network is kept 10, 20, 30, 40 and 50.

**[f]** Average End to End Delay signifies the average time taken by packets to reach from one end to another end (Source to Destination).

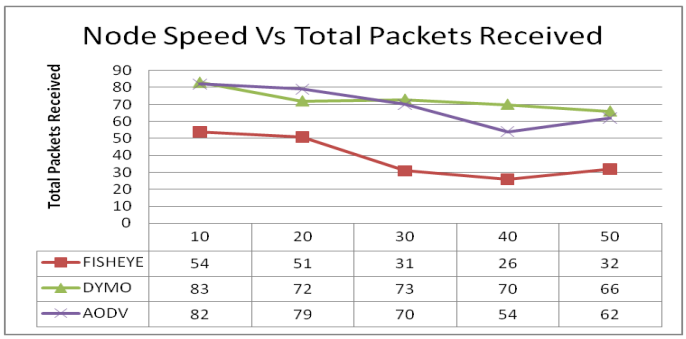



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 0.0266458 | 1.21742 | 0.0298626 | 0.0183379 | 0.0168176 |
| DYMO | 0.0824214 | 0.116854 | 0.0998185 | 0.200417 | 0.18508 |
| AODV | 0.034551 | 0.0246601 | 0.0818104 | 0.0618619 | 0.054172 |

**Figure6:-** Node Speed Vs Average End-to-End delay

Above figure shows average end-to-end delay of protocols when node speeds in network varies. It is observed that average end-to-end delay of AODV is less than FISHEYE and DYMO, when speed of node in network is kept 10, 20, 30, 40 and 50.

**[g]** A maximum packet received is the Ratio of received packets that may have been received in the network to the total number of packet sent.

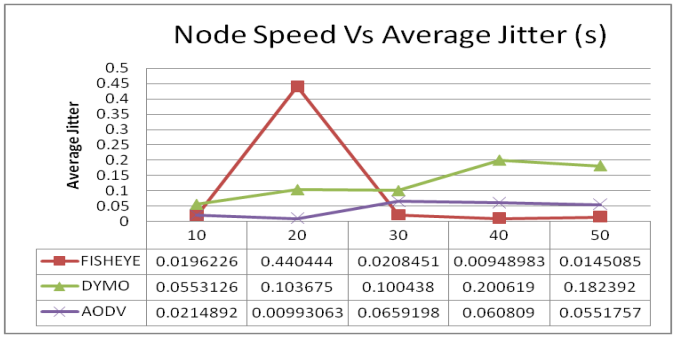



| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 54 | 51 | 31 | 26 | 32 |
| DYMO | 83 | 72 | 73 | 70 | 66 |
| AODV | 82 | 79 | 70 | 54 | 62 |

**Figure7:-** Node Speed Vs Total Packet Received

Figure 7 shows total packets received of protocols when node speed in network varies. It is observed that total packets received by network using AODV is better when speed of node is 20mps and DYMO perform better when node speed is 30 to 50 mps.

**[h]** Average Jitter effect signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.




| | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|
| FISHEYE | 0.0196226 | 0.440444 | 0.0208451 | 0.00948983 | 0.0145085 |
| DYMO | 0.0553126 | 0.103675 | 0.100438 | 0.200619 | 0.182392 |
| AODV | 0.0214892 | 0.00993063 | 0.0659198 | 0.060809 | 0.0551757 |

**Figure8:-** Node Speed Vs Average Jitter

The above figure 8 shows average jitter of protocols when node speed in network varies. It is observed that average jitter of network using AODV is less than FISHEYE and DYMO. It can be also observed that average jitter of FISHEYE is less than other protocol when speed of node in network is 30 to 50mps.

## 6. CONCLUSION

This paper presents an analysis of three routing protocols within wireless network where wormhole attack is occurred. By different analysis it can be observed that AODV performs better than other two protocols. AODV has better techniques to prevent data from attacks. In some conditions DYMO and FISHEYE performs better. But in all other conditions AODV perform better in different situations. This result gives the exact idea about the performance of AODV, DYMO, and DSR this can be helpful to enhance the performance of all above routing protocols in any situation when the wormhole attack will perform simultaneously.

## 7. REFERENCES

[1] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network", Ericsson Review, No.4, 2000, pp. 248-263.

[2] G.V.S. Raju and G. Hernandez, "Routing in Ad hoc networks," in proceedings of the IEEE– SMC International Conference, October 2002.

[3] Qualnet Simulator Documentation. "Qualnet 5.0 User`s Guide", Scalable Network Technologies, Inc., Los Angeles, CA 90045, 2006.

[4] Daniel Lang, "On the Evaluation and Classification of Routing Protocols for Mobile Ad Hoc Networks "2006.

[5] Rama Murti "Wireless Networking" 2008.

[6] Julian Hsu Julian Hsu, Sameer Bhatia, Mineo Takai, Rajive Bagrodia Performance of mobile ad hoc networking protocol in realistic scenario 2005.

[7] Existing MANET Routing Protocols and Metrics used Towards the Efficiency and Reliability- An Overview Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Ali Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia 1-4244-1094-0/07©2007 IEEE.

[8] A.Boomarani Malany 1, V.R.Sarma Dhulipala 2, and RM.Chandrasekaran 3 "Throughput and Delay Comparison of MANET Routing Protocols", Int. J. Open Problems Compt. Math.,Vol. 2, No. 3, September 2009 ISSN 1998-6262; Copyright ©ICSRS Publication, 2009 www.icsrs.org.

[9] Layuan, Li Chunlin, Yaun Peiyan "Performance evaluation and simulation of routing protocols in ad hoc networks", February 2007, Computer Communication.

[10] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540-7993/04/$20.00 © 2004 IEEE, May/June 2004.

[11] D. Djenouri, A. Derhab, and N. Badache. Ad hoc networks routing protocols and mobility. Int. Arab J. Inf. Technol.3 (2):126–133, 2006

[12] Rajiv Misra, C.R.Mandal"Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation"0-7803-8964-6/05/$20.00 lEEE 2005.

[13] A Performance Comparison of Routing Protocols for Large-Scale Wireless Mobile Ad Hoc Networks Ioannis Broustis Gentian Jakllari Thomas Repantis Mart Molle Department of Computer Science & Engineering University of California, Riverside 2004.

[14] Xin Yu, "Distributed Cache Updating for the Dynamic Source Routing Protocol," IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 609-626, Jun., 2006.

[15] Charles E.Perkins. Ad hoc Networking, Addison-Wedey, 2001.

[16] T. S. Rappaport. Wireless Communications: Principles and Practice. Prentice-Hall, 1996.

[17] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.