Performance of Ad hoc Network Routing Protocols in IEEE 802.11

Dr Chandra Shekar Reddy Putta*1,Dr K.Bhanu Prasad*2 ,Dilli Ravilla,*3
Murali Nath R.S*4,M.L.Ravi Chandra*5
Professor Coordinator, Dept. of Electronics and Communication, JNT University, Hyderabad, A.P, India[1].
Principal, Ramananda Tirtha Engineering College, Nalgonda(Dist),A.P,India[2]
Associate Professor, Dept. of Electronics and Communication, Netaji Institute of Engg. & Tech., Hyderabad, A.P[3]
Professor& Head, Dept. of Computer Science Engineering , St.Martin's Engineering College,Secunderbad, A.P,India[4].
Associate Professor, Dept. of Electronics and Communication, Netaji Institute of Engg. & Tech., Hyderabad, A.P[5]
mlravigates@gmail.com ,drpcsreddy@gmail.com Bahnu1955@37.com,
dilli.ravilla@gmail.com, Muralinath.r.s@gmail.com,

ABSTRACT: **Wireless technology based on the IEEE 802.11 standard is used to support multiple types of communication services (data, voice, and image) with different QoS requirements. Node mobility creates a continuously changing communication topology in which paths break and new one form dynamically. The routing table of each router in an adhoc network must be kept up-to-date. MANET uses Distance Vector or Link State algorithms which insure that the route to every host is always known. However, this approach must take into account the adhoc networks specific characteristics: dynamic topologies, limited bandwidth, energy constraints, and limited physical security. Two main routing protocols categories are studied in this paper: proactive protocols (e.g. Optimized Link State Routing - OLSR) and reactive protocols (e.g. Ad hoc On Demand Distance Vector - AODV, Dynamic Source Routing - DSR). The present paper focuses on study and performance evaluation of these categories using NS2 simulations. We have considered qualitative and quantitative criteria. The first one concerns distributed operation, loop-freedom, security, sleep period operation. The second are used to assess performance of different routing protocols presented in this paper. We can list end-to-end data delay, packet delivery ratio, routing load. Comparative study will be presented with number of networking context consideration and the results show the appropriate routing protocol for two kinds of communication services (data and voice).**

Keywords: performance evaluation, routing protocol, simulation, mobility.

I INTRODUCTION

MANET routing protocols are IP based and may use unicast, multicast or hybrid approaches and should allow for interaction with standard wired IP services rather than being regarded as a completely separate entity. Since the nodes in a MANET are highly mobile, the topology changes frequently and the nodes are dynamically connected in an arbitrary manner. The rate of change depends on the velocity of the nodes. Moreover, the devices are small and the available transmission power is limited. Consequently, the radio coverage of a node is small. The low transmission power limits the number of neighbor nodes, which further increases the rate of change in the topology as the node moves. Because of interference and fading due to high operating frequency in an urban environment, the links are unreliable. Ad-hoc networks are further characterized by low bandwidth links. Because of differences in transmission capacity, some of the links may be unidirectional. As a result of link instability and node mobility, the topology changes frequently and routing is difficult.

II ADHOC ROUTING PROTOCOLS

A. Routing in ad-hoc networks

A number of routing protocols have been suggested for ad-hoc networks [3]. These protocols can be classified into two main categories: proactive (table-driven) and reactive (source-initiated or demand-driven).

Pro-active protocols follow an approach similar to the one used in wired routing protocols. By continuously evaluating the known and attempting to discover new routes, they try to maintain the most up-to-date map of the network. This allows them to efficiently forward packets, as the route is known at the time when the packet arrives at the node, for example in OSPF [3].Proactive protocols are traditionally classified as either distance-vector or link-state protocols. The former are based on the distributed Bellman-Ford (DBP) algorithm, which is known for slow convergence because of the "counting-to-infinity" problem. To address the problem, the Destination-Sequenced Distance-Vector routing (DSDV) [1] protocol was proposed for ad-hoc networks. On the other hand, link-state protocols, as represented by OSPF, have become standard in wired IP networks. They converge more rapidly, but require significantly more control traffic. Since ad-hoc networks are bandwidth limited and their topology changes often, an Optimized Link-State Protocol (OLSR) [1] has been proposed. While being suitable for small networks, some scalability problems can be seen on larger networks. The need to improve convergence and reduce traffic has led to algorithms that combine features of distance-vector and link-state schemes. Such a protocol is the wireless routing protocol (WRP), which eliminates the counting-to-infinity problem and avoids temporary loop without increasing the amount of control traffic. [4]

In contrast to proactive routing, reactive routing does not attempt to continuously determine the network connectivity. Instead, a route determination procedure is invoked on demand when a packet needs to be forwarded. The technique relies on queries that are flooded throughout the network. [4]Reactive route determination is used in the Temporally Ordered Routing Algorithm (TORA), the Dynamic Source Routing (DSR) and the Ad-hoc On-demand Distance Vector (AODV) protocols. In DSR and AODV, a reply is sent back to the query source along the reverse path that the query traveled. The main difference is that DSR performs source routing with the addresses obtained from the query packet, while AODV uses next-hop information stored in the nodes of the route. In contrast to these protocols, TORA creates directed acyclic graphs rooted at the destination by flooding the route replies in a controlled manner. [4] [3]

B. proactive Vs reactive routing

Both proactive and reactive routing have specific advantages and disadvantages that make them suitable for certain types of scenarios. Since proactive routing maintains information that is immediately available, the delay before sending a packet is minimal. On the contrary, reactive protocols must first determine the route, which may result in considerable delay if the information is not available in caches. [4]

Moreover, the reactive route search procedure may involve significant control traffic due to global flooding. This, together with the long setup delay, may make pure reactive routing less suitable for real-time traffic. However, the traffic amount can be reduced by employing route maintenance schemes.

Purely proactive schemes use a large portion of the bandwidth to keep routing information up-to-date.
Because of fast node mobility, the route updates may be more frequent than the route requests, and most of the routing information is never used. Some of the scarce bandwidth is thus wasted. [4]

III DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

The key distinguishing feature of DSR is the use of source routing . That is, the sender knows the complete hop-b y-hop route to the destination. These routes are stored in a route cache. The data packets carry the source route in the packet header. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Dynamic Routing Protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad-hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach.

The difference between DSR and other on-demand routing protocols is that it is *beacon-less* and does not require *hello* packet transmissions, which are used by a node to inform its neighbors of its presence. The approach of this protocol during the route construction phase is to establish a route by flooding *Route Request* packets in the network. The destination node, on receiving a *Route Request* packet, responds by sending a *Route Reply* packet back to the source, which carries the route traversed by the *Route Request* packet received.

If a source node that does not have route to the destination and if it has data packets to be send to that destination, it initiates a *Route Request* packet. This *Route Request* packet flooded throughout the network. Each node upon receiving a *Route Request* packet rebroadcast the packet to its neighbors if it has not forwarded already or if the node is not the destination node, provided the packets time to live (TTL) counter has not exceeded. Each *Route Request* carries a sequence number generated by the source node and the path it has traversed. A node upon receiving a *Route Request* packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate *Route Request.* The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same *Route Request* by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forwarded the *Route Request* packet during the route construction phase. A destination node, after receiving the first *Route Request* packet, replies to the source node through the reverse path the *Route Request* packet had traversed.

This protocol uses a route cache that stores all possible information extracted from the source route contained in a data packet. Node also can learn about the neighboring routes traversed by data packets if operated in the *promiscuous mode.* This route cache is also used during the route construction phase. If an intermediate node receiving a *Route Request* has a route to the destination in its route cache, then it replies to the source node by sending a *Route Reply* with the entire route information from the source node to the destination node.

If any link on a source route is broken, the source node is notified using a route error (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the source route in a packet it forwards for possible future use.

IV AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

Ad-ho On-demand Distance Vector (AODV) routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by the source node for transmitting data packets. It employs destination sequence numbers to identify most recent path. The major difference between AODV and DSR stems out from that fact that DSR uses source routing in which a data packet carries a complete path to be traversed. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for the data packet transmission. In an on-demand routing protocol, the source node floods the *Route Request* packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single *Route Request*. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number to determine an up-to-date path to the destination. Anode updates its path information only if the destination sequence number of the current packet received is greater that the last destination sequence number stored at the node.

AODV shares DSR's on-demand characteristics in that it also discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers.

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route err or propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

V OPTIMIZED LINK-STATE ROUTING PROTOCOL (OLSR)

OLSR optimizes classic link state routing algorithm in which each node declares all links with neighboring nodes and floods the entire network with routing messages. OLSR protocol uses only multipoint relay nodes (MPR). So, each node maintains a table of MPR selectors and rebroadcast packets received from the originating node (MPR). Periodically, each node broadcasts"hello messages" and selects minimal subset MPR among one-hop neighbors (with symmetric link) to cover all nodes two hops away.

VI SIMULATION MODEL

A. The traffic model

In this paper we focus on Constant Bit Rate (CBR) sources (i.e voice sources) and ftp sources (i.e file transfer). The packet size is limited to 512 bytes. The source-destination pairs are chosen randomly over the network. The source-destination numbers are fixed (called connection number). We make the offered load vary by using scenarios with 10, 20,30,40,50 and 60 connections. Each source-destination pair begins packet sending at a chosen time and keeps sending between 40 and 80s for CBR sources and between 5 and 20 for ftp sources.

B. The mobility models

In this study, we focus on two mobile node mobility models to simulate their movement. First of them is the *Proba Walk* mobility model. This model uses a probability matrix to determine the node new position. Three states are used in order to determine the next position. state 0 represents the current value x or y, state 1 represents the previous x or y position and state 2 represents the mobile node next position if the mobile moves in the same direction. Each node moves using an average speed and four possible directions (ie. north, south, east, or west).

The *Proba Walk* model gives more realistic behaviors compared to random movements. The second mobility model is the *Modified Random Direction* model which was created to avoid the clustering mobile node near the center of the simulation area. This behavior occurs in the random waypoint mobility direction.

In the *Modified Random Direction* mobility model, each mobile node chooses a random direction and travels over a random distance at a random speed to it. After being arrived, it pauses for a specific time and then chooses a new direction. If it reaches the edge of the simulation area, it bounces.

C. Architectural scenarios

Some parameters are used in order to make performance evaluation of routing protocols in adhoc mobile network environment. They are resumed in the following table:

Table: THE MEAN CBR AND FTP PARAMETERS

parameters	CBR traffic	ftp traffic
node number	125,150,175,200	125,150,175,200
field size	1100	1100
simulation duration(s)	180	180
number of connections	10,20,30,40,50,60	10,20,30,40,50,60
MAC layer	IEEE 802.11	IEEE 802.11
communication range(m)	100	100
min transfer duration(s)	40	5
Max transfer duration(s)	80	20
Input rate per connection(Kb/s)	8	64

In order to simulate adhoc network with a minimum number of node's neighbors, we choose 125 as the minimum node number. The average number of neighbor nodes (NH) is given by the following equation:

$$NH=(\pi R^2/C^2)N-1$$

where R is the communication range, C is value of the field side and N is the total node number. NH is equal to 4.19 for N equal to 200.

D. Performance criteria

Three important performance metrics are evaluated:

- Packet delivery ratio: the ratio of the data packets delivered to the destination to those generated by CBR or ftp sources.
- Mean end-to-end delay: mean end-to-end delay related to data packets delivered to destination.
- Routing load: gives the number of routing packets over the number of received data packets. Each routing packet sent or forwarded by a mobile is counted.

VII RESULTS AND DISCUSSIONS

Several simulations are performed using NS2 network simulator and using parameters shown in table 1. NS2 generates a big trace files analyzed using a statistical tools developed in java. The performance study concerns three routing protocols DSR, AODV and OLSR and both CBR and ftp traffic sources.

A. Impact of traffic load

We propose here to study the impact of traffic load by varying the number of connections (pair of source-destination). The following figures show performance evaluation of AODV, DSR and OLSR protocols related to 10, 20, 30, 40, 50 and 60 connections and 200 mobile nodes. In authors show that the mobility models may drastically affect protocol performances. So, using the *Proba Walk* mobility model was conducted by study walker scenarios aim in this part of a paper. We first observe in figure 1 that AODV outperform DSR and OLSR for packet delivery ratio (3 to 5% compared to OLSR) and also routing load criteria as shown in figure 5 (between 4 and 12 times lower). As shown in figure 3, OLSR performs better and gives little variation when the traffic load increases. Until 30 connections, all studied routing protocols perform identically but when the traffic load increases, OLSR performs better for delay. However, routing load is higher (see figures 5 and 6) because it periodically sends routing packets in order to maintain the routing table up-to-date. As shown in figures 2 and 4, DSR seems to produce higher percentage of data packets for ftp sources even if it produce higher delay. We also observe packet delivery ratio higher (about 98%) compared to CBR sources because ftp uses TCP protocol which insures packets retransmission when dropped.

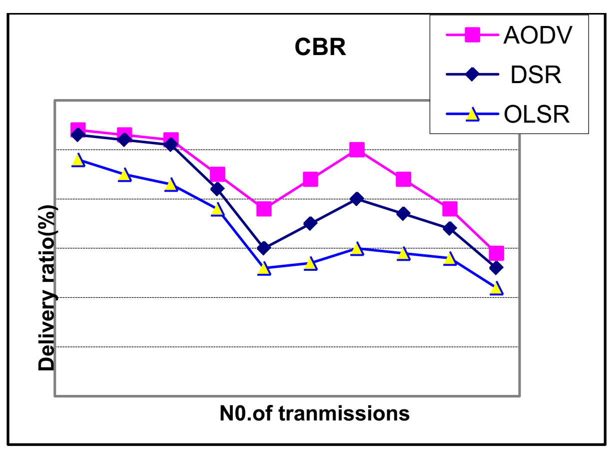

Figure 1: N-200, Proba Walk mobility model

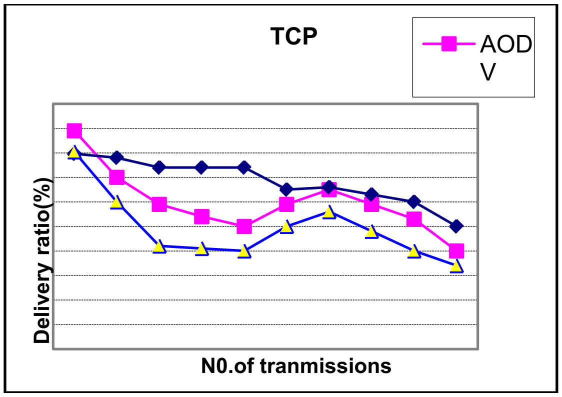

Figure 2: N-200, Proba Walk mobility model

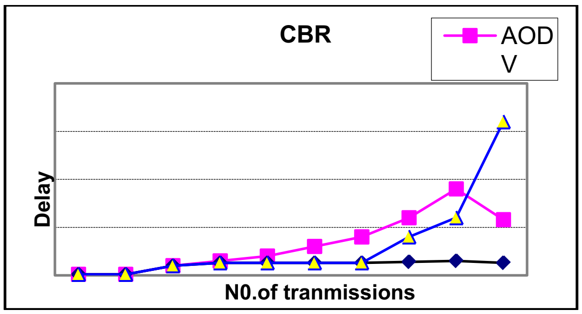

Figure 3: N-200, Proba Walk mobility model

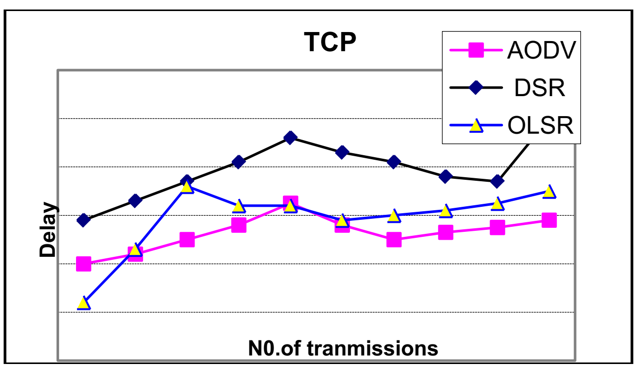

Figure 4: N-200, Proba Walk mobility model

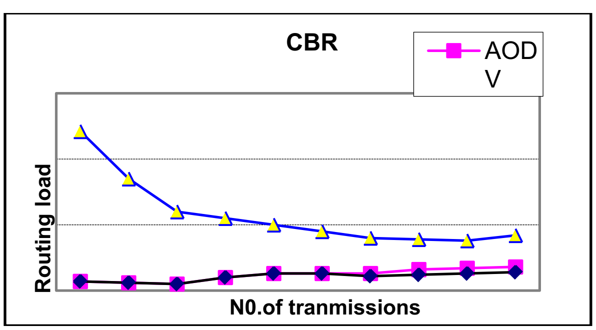

Figure 5: N-200, Proba Walk mobility model

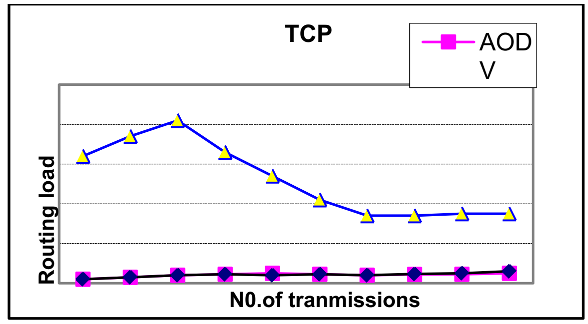

Figure 6: N-200, Proba Walk mobility model

B. Impact of mobile node mobility

In order to study the impact of the node mobility against adhoc routing protocols, we have pitched on the *Modified Random Direction* mobility. The mean feature of the model is travelling on all simulation area which avoiding nodes centralization in a specific zone.

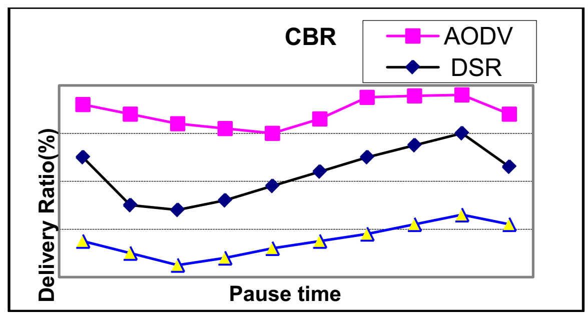

Fig7: 40 connections, Modified Random Direction mobility model

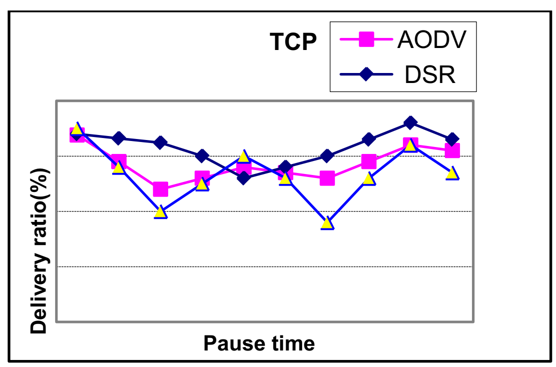

Fig8: 40 connections, Modified Random Direction mobility model

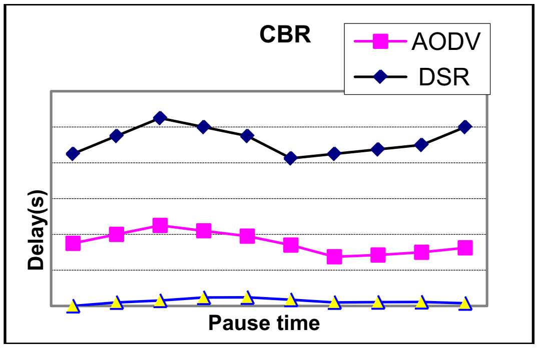

Fig9: 40 connections, Modified Random Direction mobility model

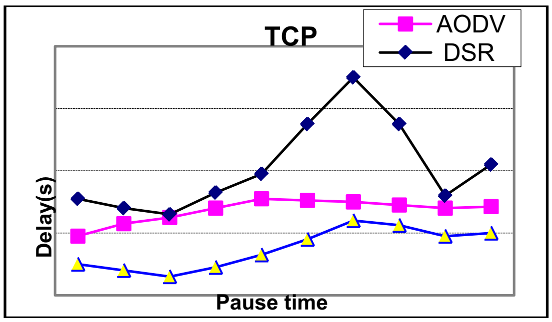

Fig10: 40 connections, Modified Random Direction mobility model

Figure: 7 show the small increases of packet delivery ratio when the mobility decreases (pause time increases between 10 and 20).The files transfer are delay sensitive while the packet delivery ratio criteria is much more important QoS. In this case, DSR and AODV seem to be quite identical. (see figures 7 and 9).

VIII CONCLUSIONS

In this paper we have evaluated the performance of reactive (ie. DSR and AODV) and proactive (ie. OLSR) routing protocols in 802.11 adhoc network environment. We have noticed the proactive protocol (OLSR) offers better performances for CBR sources (eg. voice services) given that it guaranties lowest delay. However it consumes much more bandwidth. Periodically, OLSR protocol sends routing packets to discover and to maintain routes to all destinations. That's why the number of delivered packets decreases when the traffic load (number of connections) increases. For 10 connections, the packet delivery ratio is about 53 %. The reactive routing protocols are more adapted for data services (file transfer). They guarantee a packet delivery ratio of 80% for 60 connections (480 kbit/s). There is no clear winner among DSR and AODV since routing load and delay are quite identical. We have also pointed out the influence of the node mobility model on the adhoc routing protocols. In *Proba Walk* mobility, direction range is indeed more limited than in *Modified Random Direction* model.

REFERENCES

[1] C. Perkins, E. Royer, S. Das and K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks,"' in IEEE Personal Communications, February 2001.

[2] Clausen, T., Jacquet, P., Laouiti, A., Minet, P., Qayyum, A., Viennot, L.: "Optimized Link State Routing Protocol", Sept 2001, IETF Internet Draft, draft-ietf- manet-olsr-06.txt

[3] Perkins, C. E., Royer, E. M.: "Ad-hoc On-Demand Distance Vector Routing", February 1999, Proc. 2nd IEEE Workshop on Mobile Computer Systems and Applications, pp. 90-100

[4] Fan Bai, Narayanan Sadagopan , Ahmed Helmy, "The IMPORTANT framework for analyzing the Impact of Mobility on Performance Of RouTing protocols for Adhoc NeTworks", INFOCOM, 2003.

[5] Tracy Camp, Je Boleng, Vanessa Davies, "A survey of mobility models for adhoc network research", Wireless communications and mobile computing, volume 2, Issues 5, page 483-502, 2002.

[6] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", draft-ietf-manet-olsr-11.txt, july2003.

[7] David B. Johnson, David A. Maltz, Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile AdHoc Networks (DSR)", draft-ietf-manet-dsr- 10.txt, july 2004.

[8] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", draft- ietf-manet-aodv-13.txt, february 2003.

[9] Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K. Tripathi, "A framework for reliable routing in mobile adhoc networks", infocom, 2003.

[10] Santashil PalChaudhuri and Sridhar Lavu. A perfomance comparison of ad hoc network routing protocols. Rice University, 2000.

[11] Shreee Murthy and J.J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. University of California, 1996.

[12] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. Colorado School of Mines, 2002.

[13] Fan Bai, Narayanan Sadagopan, and Ahmed Helmy. User manual for IMPORTANT mobility tool generators in NS-2 simulator. University of Southern California, 2004.

[14] ANSI/IEEE Std 802.11, 1999 edition - Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE, 1999.

[15] Philippe Jacquet, Paul Muhlethaler and Amir Qayyum,"Optimized Link State Routing Protocol". Internet draft, draft-ietf-manet-olsr-00.txt, November 1998.

[16]David B. Johnson and David A.Maltz, "Dynamic source routing in ad hoc wireless networks". In *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.

[17] Josh Broch, David B. Johnsson, David A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks". Internet Draft, draft-ietf-manet-dsr-00.txt, March 1998. Work in progress.

[18] S.R. Das, R. Castaneda, J. Yan, R. Sengupta, Comparative Performance Evaluation of Routing Protocols for Mobile Ad hoc Networks, Proceedings of the 7th International Conference on Computer Communications and Networks, 1998, pp. 153-161.

[19] Ad-hoc distance vector protocol(AODV) for mobile ad hoc network http://www.olsr.org/docs/ #adhoc_aodv#adhoc_aodv –accessed on may 2009.

[20]. RFC 3626 (OLSR) Optimized Link State Routing. http://www.ietf.org/rfc/rfc3626.txt

[21]. RFC 3561 (AODV) Ad hoc On Demand Distance Vector. http://www.ietf.org/rfc/rfc3561.txt

[22]. (DSR) Dynamic Source Routing. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[23] Network Simulator (NS2), http://www.isi.edu/nsnam/ns.