Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols

Amit Shrivastava
Aravinth Raj Shanmogavel
Avinash Mistry

Nitin Chander
Prashanth Patlolla
Vivek Yadlapalli

Department of Computer Science
Lamar University
P.O.Box 10056
Beaumont TX 77710
E-mail : lamarseminar2005@yahoogroups.com

Abstract
A mobile ad-hoc network (MANET) is a self starting dynamic network comprising of mobile nodes, where each and every participation node voluntarily transmit the packets destined to some remote node using wireless (radio signal) transmission. An ad hoc network doesn't have any centralized arbitrator or server. In MANET each and every mobile node is assumed to be moving with more or less relative speed in arbitrary direction. Because of that there is no long term guaranteed path from any one node to other node. MANET have very enterprising use in emergency scenarios like military operations & disaster relief operation where there is need of communication network immediately following some major event, or some temporary requirement like conference & seminar at new place where there is no earlier network infrastructure exist and need alternative solution.

1. Introduction

"Wireless networking is a technology that enables two or more computers to communicate using standard network protocols, but without network cabling" [9]. And now there exist network protocols that are developed just for the purpose of Wireless networks. We can categorize wireless network in primarily following two categories.

a) Network with existing infrastructure: is a network where exists a wireless access point or earlier wireless hardware support for each node to connect to networks. Here nodes do not participate in any kind of transit services. They communicate to access points to send & receive packets from other nodes. In this kind of network different access point can follow different wireless protocol like 802.11 b or 802.11g and still can communicate with each other. There exist several wireless products based on this kind of technology.

b) Ad hoc network is a network where there is no existence of wireless infrastructure for networking, Instead each node communicates with each other using their sole transmitter-receiver only. In this kind of network each and every node does participate voluntarily in transit packet that flow to and from different nodes. Each node do follow same routing algorithm to route different packets. Thus this kind of network have limited homogenous feature. There are not many wireless products that follow this proposed technology.

2. Mobile ad-hoc network (MANET)

"A mobile ad-hoc network(MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links." [11].
Some of the main features of MANET are listed below [2]:

a) MANET can be formed without any preexisting infrastructure.
b) It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network.
c) It does have very limited physical security, and thus increasing security is a major concern.
d) Every node in the MANET can assist in routing of packets in the network.
e) Limited Bandwidth & Limited Power.

2.1. Security in MANET

There is very limited physical security in MANET. The type of attacks can be Active attacks or Passive attacks [5]. The common security issues are Passive attacks which include eavesdropping and information disclosure. Active attacks include Denial of service, Data modification by viruses, Trojans and worms.

There are other more specific problems with mobile ad hoc network such as vulnerability of channels and nodes, Byzantine black hole and Byzantine wormhole attack [1]. The security issue also include attacks that may inject erroneous routing information and diverting network traffic thus making routing inefficient.

There are many methods to reduce the impact of these attacks, which include a secure routing using public and private keys to get a certification authority and use of digital signatures and priori trust relationships. The drawbacks of such a system is that the priori trust needs to be in place before the network is set up this may not always be possible in a case of disaster affected areas[5, 8].

In this project we try to see how DSR protocol implementation with the Watchdog extension can help to mitigate attacks on routing in ad-hoc networks by detecting some malicious nodes and how the Pathrater addition to the DSR can make routing more efficient.

3. Routing in MANET

"Routing is the process of information exchange from one host to the other host in a network."[4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself [2].

3.1 Different Strategies

Routing protocol for ad-hoc network can be categorized in three strategies.
a) Flat Vs Hierarchical architecture.
b) Pro- active Vs Re- active routing protocol.
c) Hybrid protocols.

3.2 Flat Vs. Hierarchical architecture

Hierarchical network architecture topology consists of multiple layers where top layers are more seen as master of their lower layer nodes. There are cluster of nodes and one gateway node among all clusters has a duty to communicate with the gateway node in other cluster. In this schema there is a clear distribution of task. Burden of storage of network topology is on gateway nodes, where communicating different control message is dependent on cluster nodes.

But this architecture breaks down when there is single node failure (Gateway node). Gateway nodes become very critical for successful operation of network. Examples include Zone-based Hierarchical Link State (ZHLS) routing protocol [6]. Where in flat architecture there is no layering of responsibility. Each and every node does follow the same routing algorithm as any other node in the network.

3.3 Proactive Vs Reactive routing protocol in MANET

3.3.1Proactive routing protocol

In proactive routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology.

Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment.
Destination Sequenced Distance Vector Routing protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm.

Examples of Proactive Routing Protocols are: [7].
a) Global State Routing (GSR).
b) Hierarchical State Routing (HSR).
c) Destination Sequenced Distance Vector Routing (DSDV).

3.3.2 Reactive routing protocol

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network topology may break active route and cause subsequent route search [6].

Examples of reactive protocols are:
a) Ad hoc On-demand Distance Vector Routing (AODV).
b) Dynamic Source Routing (DSR).
c) Location Aided Routing (LAR).
d) Temporally Ordered Routing Algorithm (TORA).

3.4 Hybrid routing protocols in MANET

There exist a number of routing protocols of globally reactive and locally proactive states. Hybrid routing algorithm is ideal for Zone Based Routing Protocol (ZRP) [6].

3.5 Cost benefits trade-off between proactive and reactive protocols

Advantage: proactive Vs reactive

Proactive protocols: Routes are readily available when there is any requirement to send packet to any other mobile node in the network. Quick response to Application program.

Reactive protocols: These are bandwidth efficient protocols. Routes are discovered on demand basis. Less Network communication overhead is required in this protocol.

Disadvantage: proactive Vs reactive

Proactive protocols: These maintain the complete network graph in current state, where it is not required to send packets to all those nodes. Consumes lots of network resources to maintain up-to-date status of network graph. "A frequent system-wide broadcast limits the size of ad-hoc network that can effectively use DSDV because the control message overhead grows as $O(n^{2})$." [2].

Reactive protocols: These have very high response time as route is needed to be discovered on demand, when there is some packet to be send to new destination which does not lie on active path.

4. Reactive routing protocols

Reactive routing protocols are more popular set of routing algorithms for mobile computation because of their low bandwidth consumption.

4.1 AODV

AODV stands for Ad-hoc On demand Distance Vector. AODV is distance vector type routing where it does not involve nodes to maintain routes to destination that are not on active path. As long as end points are valid AODV does not play its part. Different route messages like Route Request, Route Replies and Route Errors are used to discover and maintain links. UDP/IP is used to receive and get messages.. AODV uses a destination sequence number for each route created by destination node for any request to the nodes. A route with maximum sequence number is selected. To find a new route the source node sends Route Request message to the network till destination is reached or a node with fresh route is found. Then Route Reply is sent back to the source node. The nodes on active route communicate with each other by passing hello messages periodically to its immediate neighbor. If a node does not receive a reply then it deletes the node from its list and sends Route Error to all the members in the active members in the route. AODV does not allow unidirectional link [3]. Finally the animator in any simulation has to be discussed. NAM is used in NS2.

4.2 DSR

This is an On-demand source routing protocol. In DSR the route paths are discovered after source sends a packet to a destination node in the ad-hoc network. The source node initially does not have a path to the destination when the first packet is sent. The DSR has two functions first is route discovery and the second is route maintenance [5, 8].

4.2.1 Different DSR Algorithms

a) Route discovery.
b) Route maintenance.

Assumptions:

a) X , Y, Z , V and W form ad-hoc network.
b) X is the source node.
c) Z is the destination node.

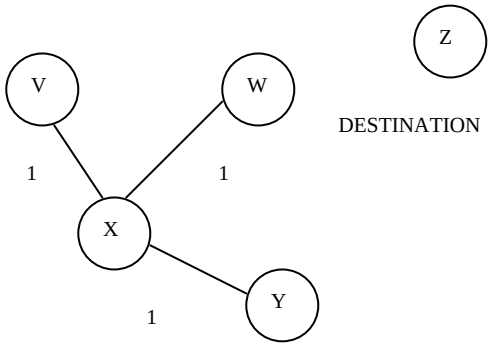

Fig.1. DSR algorithm routing process.

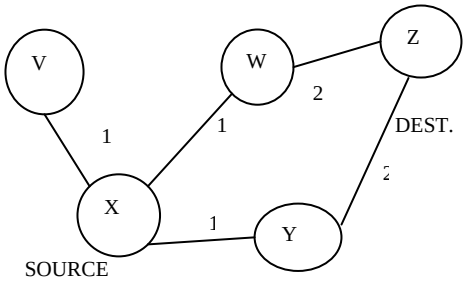

Fig.2. showing re-broadcasting by nodes V, W, Y.

Route discovery algorithm [5, 8]:

a) X broadcasts a Route Request Packet with the address of destination node Z.
b) The intermediate nodes V, W, Y receive the Route Request Packet from X, as shown in Fig1.
c) The receiving nodes V, W, Y each append their own address to the Route Request Packet and broadcast the packet further as shown in Fig2.
d) The destination node Z receives the Route Request packet. The Route Request packet now contains

information of all the addresses of nodes on the path from the source node X to the destination node Z.

e) On receiving the Route Request Packet the destination node Z sends a reply called the Route Reply Packet to the source node X by traversing a path of addresses it has got from the Route Request packet.
f) DSR caches the route information for future use.

Route Maintenance algorithm [5, 8]:

a) In DSR algorithm a link break is detected by a node along the path from node X to node Z, in this case node W.
b) Then node W sends a message to source node X indicating a link break.
c) In this case, node X can use another path like X-Y- Z or it must initiate another route discovery packet to the same destination node, in this case 'Z'.

4.2.2 DSR Watchdogs [8]

The main function of watchdog is to detect misbehaving nodes. The advantage of this method is that it detects failures not only at link level but also at the forwarding level. This algorithm works good with source routing protocols since the hop-by-hop nature of DSR. Without DSR, the watchdog would not know about a message lost due to a broken link. [8].

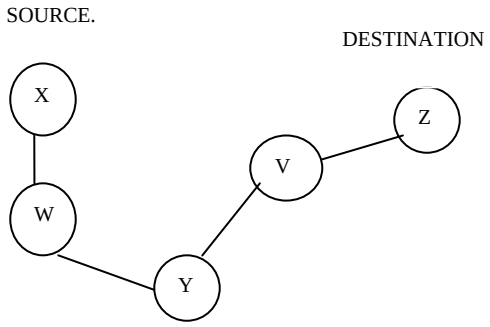

Fig.3. Watchdog reference figure.

Assumptions:

a) Nodes X, W, V, Y, and Z form an ad-hoc network.
b) Nodes X is the source node
c) Node Z is the destination node
d) Nodes W,Y,V are the intermittent nodes
e) Node W can transmit to and receive from Y and X only, and not to or from the other nodes.
f) Node Y can transmit to and receive from W and V only, and not to or from the other nodes.
g) Node V can transmit to and receive from Y and Z only, and not to or from the other nodes.
h) Each node maintains a buffer that holds the recently transmitted packets by that node.

Watchdog Algorithm:

a) Once a node sends a packet to some other node it also adds it to its Buffer i.e. if X sends a packet to W it will add the packet to its own buffer.
b) The node that sent the packet, node X, listens for its neighbor transmissions, node W's transmissions. Node X then compares the overheard packet to the packet in its own buffer.
c) If the packet in the buffer of node X matches the packet transmitted by node W then the packet is removed from buffer of node X.
d) If the packet doesn't match and if the packet in the buffer of any node exceeds a timeout then a tally is incremented for the node that is to transmit the packet.
e) If this tally is greater than the misbehavior threshold then it is said to be a misbehaving node and a message is sent to node X (i.e. the source node) by the misbehaving node to inform it of the misbehaving node.

4.2.3 The DSR with Pathrater

Pathrater decides the route of packets from one node to another in an Ad-hoc network. Pathrater uses knowledge of misbehaving nodes reported by watchdog and also the link reliability data that it is going to maintain for route selection. Each node maintains another node's rating information, termed as metric, depending upon the packet dropping and packet sending to other nodes successfully. The exact path the packet has traversed has to be known by pathrater hence it should be implemented on top of source routing protocol [1].

Assumptions:

a) All the assumptions are similar to one described in watchdog in section 4.2.2.

Algorithm to choose a route:

a) Each node in the pathrater maintains rating of every other node in the Ad-hoc network.
b) Path metric is calculated by taking average of the ratings of each node in the path as this allows pathrater to choose shortest path algorithm if no metric is given to nodes.
c) In case of multiple paths a route with highest metric is chosen [1].

Pathrater differs from DSR algorithm because DSR depends on shortest path algorithm [1].

Algorithm for assigning rating to a node:

a) For a neutral node, that is a new node that pathrater just comes to know, is given a rating of 0.5.
b) Rating of each node is done with top rating of 1.0 to ensure if all are neutral nodes then shortest path first is chosen.
c) For every 200ms the rating of nodes on active path is incremented by 0.01.
d) Maximum value of neutral node is 0.8.
e) Packet is dropped on a link and if a node becomes un-reachable will lead to deduction of 0.05 of node's rating.
f) Lower limit of a neutral node is 0.0.
g) Changes on the ratings of other nodes than one mentioned above are not performed.
h) Any misbehaving node reported by watchdog is given a rating of -100.
i) If the simulation is run for long period of time then the negative ratings can be reset after a long timeout period.
j) If no node is found that can be given packet to forward, Send Route Request is given [1].

4.2.4. Different caching techniques in DSR

Each mobile host participating in the ad hoc network maintains a route cache in which it caches the source route that it has learned. There are several techniques for a node to learn & store about the route, some of them are as follows.

a) Running network interface in promiscuous mode.
b) Reading the route information from data packets.
c) Reading the routing information from Route Discovery packets.
d) Reading the broken route information from Error packets.

There are three different caching design strategies to be considered.

4.2.4.1. Cache structure

There are two basic cache structures to select from for ad hoc network

a) Path cache.
b) Link cache.

Path cache is very simple to implement and also guarantees loop- free nodes but it do not effectively utilize all of the potential information that node might learn about the state of the network. On other side, link cache has do need Dijkstra's shortest-path algorithm to find the current best path through the graph to the destination node, and it also do have loop in the path.

4.2.4.2. Cache capacity

For a link cache, we need to store the entire path that is discovered. If network has N different active nodes then there is at max N^2 different paths to store. While a path cache need much larger storage space as there is no common nodes or common path stored among different paths.

In addition we can add two levels in Cache design:

a) Primary cache.
b) Secondary cache.

Primary cache store the paths that has been used by this node after it has learned about them, while the secondary cache store the paths that has not been used ever since node learned about them.

4.2.4.3. Cache timeout

There are two different timeout strategies that can be adopted:

a) Static timeout.
b) Adaptive timeout.

Static timeout assigns constant time out period for each entry after that path were used last time and it is decremented with every time pulse. While in adaptive timeout the path that has been used more frequently are assigned longer weighed timeout period.

4.2.4.4. Caching algorithm

There are two different caching algorithms and their selection is directly dependent on caching structure.

a) Path cache (path-Inf, FIFO-64, FIFO- 32, Gen-34).
b) Link cache (NoExp, Adapt-1.25, MaxLife).

4.2.4.5. Mobility prediction in DSR

"The destination predicts the change in topology ahead of time and determines when the flow needs to be rerouted or 'handoffed' based on the mobility information contained in the data packets." [10].

This proposed improvement in protocol uses network's current knowledge about the reliability of different links and predicts the expiration time for different links based on their past caching. It selects the more reliable route, in terms of Route Expiration Time (RET), when there are multiple paths available with different number of hops to forward the packet. It is probabilistic approach and has certain advantage in current simulation results.

4.3. Location Aided Routing (LAR)[12]

LAR uses the basic flooding algorithm that is defined in DSR with the exception that it uses location information of a particular node to limit the flooding in the network. The location information can be gathered using the Global Positioning System (GPS).Some times the GPS might only give the approximate location of a node. Even then the LAR protocol can be used. Using the location information, LAR calculates the expected zone of a particular node.

4.3.1. Expected Zone [12]

In a MANET, the nodes will be moving. So, the expected zone is the zone in which a particular node is expected to be at that particular instance of time.
For example, if node D is at a location L at time t0 and node D is moving with a speed v. Then at time t1, node D is expected to be in a circular region with radius v (t1-t0) from the location L.

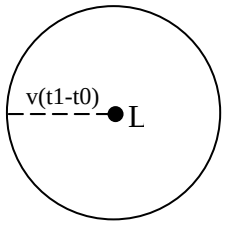

Fig.4. Expected Zone

If a node S wants to calculate the expected zone of node D, node S should know the location of node D at time t0 and the speed at which the node D is moving. With out knowing any one of these details, node S cannot calculate the expected zone of node D and hence assumes the entire ad hoc network to be the expected zone. The speed can be the average speed, maximum speed or any other measure related to the speed.

4.3.2. Request Zone [12]

LAR limits flooding using the request zone i.e., in LAR, a node forwards a packet if it is in the request zone and discards the packet if it is not in the request zone.
For example, if node S needs to find a route to node D. Then node S calculates the request zone and broadcasts the values of the zone along with the packet. A node that is receiving the packet that is sent by S only broadcasts the packet again if it is in the request zone and it is not the intended destination node.
A request zone should include the expected zone of the destination and may include other regions because, if a sending node S is not in the expected zone of destination node D, then the request zone should include both S and expected zone of D as follows.

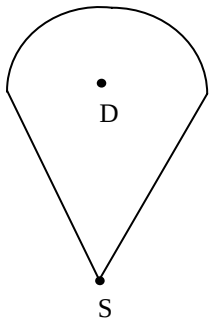

Fig.5. Request Zone [12]

But if none of the other nodes through which the packets have to travel are not in the request zone as above then you may need to expand the request zone. The below two pictures depicts this.

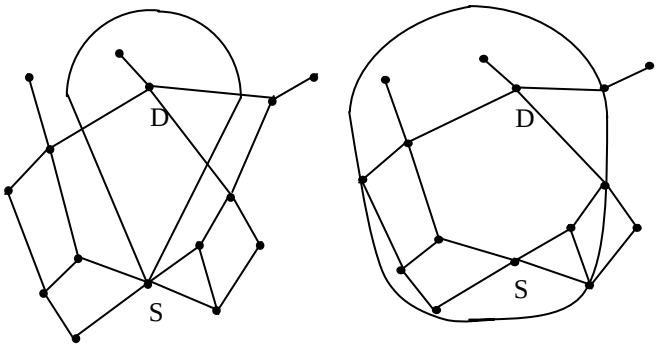

Fig.6. Expanded Request Zone [12]

There are two schemes proposed in LAR to determine if a node is in the request zone or not. They are as follows.

4.3.3. LAR Scheme1 [12]

In LAR Scheme1, node S first calculates the request zone for the node D and broadcasts the co-ordinates of the request zone along with the route request packet. The request zone is rectangular in shape and the co-ordinates are calculated by drawing a smallest rectangle that includes the current location of S and the expected zone of D such that the sides of the rectangle are parallel to the X and Y axes. An intermediate node checks the co-ordinates in the packet and broadcasts if it is in the request zone. All other nodes that are not in the request zone discard the packet. If none of the nodes are in the request zone that is calculated by S, the packet is not sent to D and henceforth S doesn't get the reply back. Then S increases the size of the request zone which is the whole ad hoc network.

The figure below shows when S not in the expected zone of D. S calculates the co-ordinates S, A, B and C and includes them along with the packet.

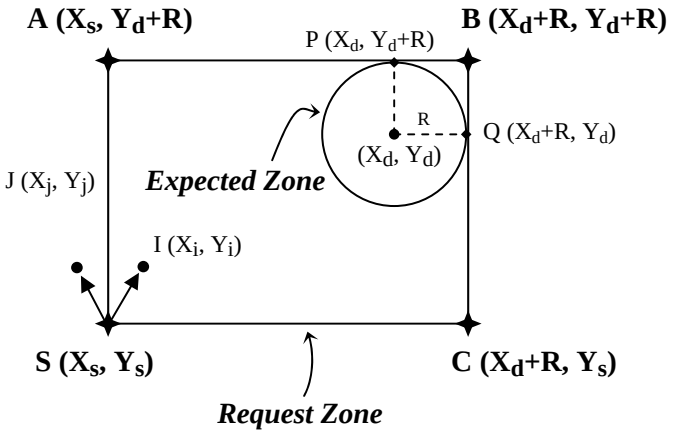

Fig.7. LAR Scheme1. Co-ordinates out side expected zone [12]

The figure below shows when S is in the expected zone of D and the co-ordinates G, A, B and C are calculated and included along with the packet.

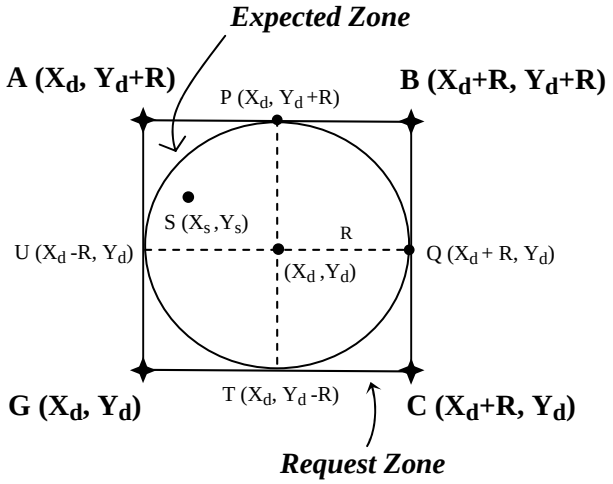

Fig.8. Co-ordinates when S is in the expected zone [12]

4.3.4 LAR Scheme 2 [12]

Unlike in LAR Scheme1, LAR Scheme2 doesn't include the co-ordinates of the request zone but it rather includes two other pieces of the information. Assuming that S knows the location of D, S calculates the distance it is from D and includes the distance and the co-ordinates of D along with the route request packet. Whenever an intermediate node receives this packet, it forwards the packet only if it is not farther than the distance provided in the packet. While forwarding it replaces the previous distance by its own distance to the destination.

For example, if node S is initiating the route discovery to node D and S knows the location information of D i.e., (X_d, Yd), S calculates its distance from D, lets say $DIST_s$. S sends DISTs and (X_d,Y_d) to all its neighboring nodes. When neighboring node I received the packet, it calculates its distance $DIST_i$ from (X_d,Y_d) and

1. For some parameters g and h if g ($DIST_s$) +h>= $DIST_i$ then node I will replace $DIST_s$ by $DIST_i$ in the packet and broadcasts it to its neighbors.
2. If g ($DIST_s$) +h< $DIST_i$ then node I will discard the packet.

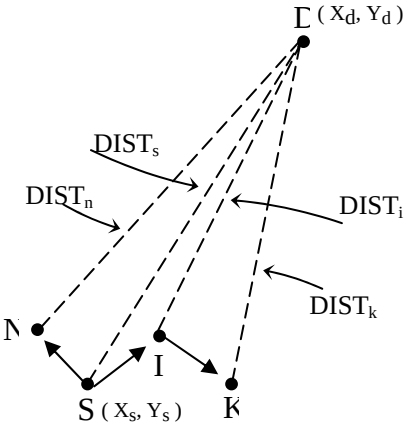

Fig.9. LAR Scheme 2 [12]

5. Conclusion

Wireless mobile ad-hoc network has very enterprising applications in today's world. With fast growing technology mobile laptop computers and wireless hardware costs are becoming very affordable. There is increasing use of wireless devises. Sales of mobile laptop will outperform sales of desktop computers by the end of year 2006 [Communication Magazine, Sep-2004]. Reactive protocols are active research area in the field of ad-hoc mobile network. There are still lots of simulations to be done in this promising field.

References

[1] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens *"Mitigating Byzantine Attacks in Ad Hoc Wireless Networks"*, ACM MobiCom, Aug-2000.

[2] Charles E.Perkins and Elizabeth M. Royer, *"Ad hoc on demand distance vector (AODV) routing (Internet-Draft)*", Aug-1998.

[3] Eitan Altman and Tamia Jimenez, *"NS for Beginners"*, http://www-sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS/n3.pdf, Jan-2002.

[4] Humayun Bakht, "*Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks"*, http://www.computingunplugged.com/issues/issue200410/00001395001.html, April-2003.

[5] Loutfi, Valerie, Bruno. "*Securing mobile adhoc networks"*, MP71 project, 2003

[6] Mario Joa-Ng, "*A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks*", IEEE Journal on selected areas in communications, Vol. 17, No. 8, Aug-1999.

[7] Padmini Misra, *"Routing Protocols for ad hoc mobile wireless Networks"*, http://www.cse.ohio-state.edu/~jain/cis788-99/ftp/adhoc_routing/#TDRP, Nov-1999.

[8] Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker *"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks"*, Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, Massachusetts, 2000,Pages: 255 - 265

[9] Vicomsoft, "*Knowledge share whitepapers wireless networking Q&A*", Vicomsoft connect and protect, Jan 2003

[10] Williams Su, Sung-Ju Lee and Mario Gerla, "*Mobility prediction and routing in ad hoc wireless networks*", International journal of network management, 2001; 11:3-30

[11] Wikipedia, *"The free encyclopedia-, Mobile ad-hoc Network"*, http://en.wikipedia.org/wiki/Mobile_ad-hoc_network, *Oct*-2004.

[12] Young-Bae Ko and Nitin H. Vaidya, "*Location-Aided Routing (LAR) in mobile ad hoc networks*", Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking**,** Dallas, Texas, 1998, Pages: 66 - 75