International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-3, May-2014

Review of MANETs

Rashmi Makkar, Ms. Suman Sangwan

Abstract- **MANET is a decentralized autonomous system in which different nodes are connected to each by wireless links. Nodes in the network can be either fix or mobile. Mobile nodes may include laptop, mobile phones, MP3 Player. Nodes may be located on ships, airplanes, land irrespective of their location as they can participate in communication. To facilitate the communication within the network, a routing protocol is used to discover the routes between nodes. The primary goal of such an network routing protocol is correct and efficient route establishment between a pair of nodes so that message can be deliver in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption. This paper provides an overview of different Geographical routing protocols with their merits and drawbacks.**

I. INTRODUCTION

Wireless network has become very popular in the computing industry. Wireless network are adapted to enable mobility. There are two variations of mobile network. The first is infra-structured network (i.e. a network with fixed and wired gateways). The bridges of the network are known as base stations. A mobile unit within the network connects to and communicates with the nearest base station (i.e. within the communication radius). Application of this network includes office WLAN. The second type of network is infrastructure less mobile network commonly known as AD-HOC network. They have no fixed routers. All nodes are capable of moving and be connected in an arbitrary manner. These nodes function as routers, which discover and maintain routes to other nodes in the network. Non infrastructure based MANET are expected to become an important part of the 4G architecture. Ad-hoc networks can be used in areas where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Some applications of ad-hoc network are students using laptop to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information about situation awareness in a battlefield, and emerging disaster relief after an earthquake or hurricane. Ad hock networks are created, for example, when a group of people come together and use wireless communication for some computer based collaborative activities; this is also referred to as spontaneous networking.

An ad-hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support services regularly available on conventional networks. The nodes are free to move randomly and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably. Such a network may operate in standalone fashion, or may be connected to the larger internet. Mobile ad-hoc networks are infrastructure less networks since they do not require any fixed infrastructure such as a base station for their operation. In general routes between nodes in an ad-hoc network may include multiple hops and hence it is appropriate to call such networks as "multi-hop wireless ad-hoc networks". Each node will be able to communicate directly with any other node that resides within the transmission range. For communication with nodes that reside beyond this range the node needs to use intermediate nodes to relay the messages hop by hop.

Generally there are two distinctive approaches for mobile nodes to communicate with each other:

A. ***Infrastructure Based Networks*** : In this network, base station are connected to fixed network infrastructure and communicate to other nodes via that fixed base station. Example – WLAN, WLL, UMTS.

Fig 1: Infrastructure Base Networks

B. ***Infrastructure less Networks****:* As in adhoc network each node can communicate with other node dynamically without using any fixed predefined infrastructureso it can implement in the places where no infrastructure exists. Thus making it useful for it an application in disaster recovery situations where instant communication is required

Manuscript received May 21, 2014
Rashmi Makkar, Panipat, Haryana, India (makkar.rashmi21@gmail.com)
Ms. Suman Sangwan, Panipat, Haryana, India (suman2222@yahoo.com)

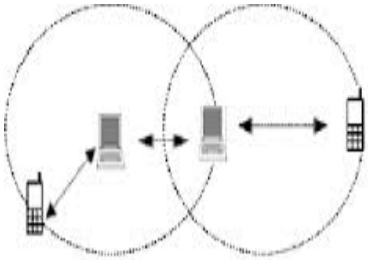


Fig 2: Infrastructure Less networks

II. MANET APPLICATIONS

MANET is implemented in several fields, discussed below:

A. **Crisis Management Application**: Natural disaster are unpredictable and require quick response with in a time constraint. As a result of natural disaster in which entire communicaton infrastructure is in disarray. Restoring communication fastly becomes essential in that case. With Wide Band Wireless communication, Internet and video services could be setup in hours instead of days.

B. **Education via Internet**: Educational opportunity available to internet, individuals interested in life long education could be unavailable to clientle living in thinly popoulated or remote areas because of economic infeasibility of providing wireline internet access in these areas to our subscribers. So wireless communication provides access in even thinly populated area to the users.

C. **Telemedicine:** The paramedic assisting the victim of traffic accident in a remote location must have access medical records and may need video conferencing for assisting surgeons during operation or emergency intervention.

D. **Civilian Applications:** Using wireless network alarms can be activated for various disaster situations suggest forest fire, flood and precision agriculture which enables quick reaction before situation becomes uncontrollable.

E. **Troposbased Mesh Technology:** Using this technology we can cover an area of more than Eight square miles making use of several access points, of which less than 20% of them are connected using backhaul network. This reduces the network installation cost and makes its implementation cost effective in rular or scarcely populated areas.

F. **Sensor Networks**: They consist of large no. of small sensors, which can be used to detect temperature, pressure, toxins and pollution of an area. The capability of each sensor is very limited and they rely on others in order to forward data to a central computer. Individual sensors doing this are pron to failure and lose.

G. **Wildlife monitoring:** Wildlife monitoring is an interesting application field for opportunistic networks. It focuses on tracking wild species to deeply investigate their behavior and understand the interactions and influences on each other, as well as their reaction to the ecosystem changes caused by human activities. Researchers use opportunistic networks as a reliable, cost-effective, and not intrusive means to monitor large populations roaming in vast areas. Systems for wildlife monitoring generally include special tags with sensing capacity to be carried by the animals under study, and one or more base stations to collect the data from the tags and send them to the destination processing centre. A network protocol is also comprised to percolate the data from the tags towards the base station(s). Base stations can be fixed or mobile, however, in both cases data collection from all the deployed tags is quite challenging. Therefore, it is generally advisable to exploit pair-wise contacts between the animals to let them exchange the information already collected. As a consequence, each animal eventually carries the information collected by its own together with the information collected by the animals it has encountered. The realistic projects include ZebraNet at Princeton University which is used for tracking zebras wearing special collars and SWIM (Shared Wireless Infostation Model) which is used to monitor whales.

H. ***Monitoring the aquatic environment:-*** The underwater wireless sensor network have applications including the scientific (e.g., oceanographic data collection for scientific exploration, pollution control, or climate monitoring), military (e.g., tactical surveillance), and civilian fields (e.g., tsunami warnings).

I.

III. MANET CHALLENGES

1) ***Limited bandwidth*****:** Wireless link continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

2) ***Dynamic topology***: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

3) ***Routing Overhead***: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

4) ***Hidden terminal problem*****:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not

within the direct transmission range of the sender, but are within the transmission range of the receiver.

5) ***Packet losses due to transmission errors*****:** Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.

6) ***Mobility-induced route changes*****:** The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

7) ***Battery constraints*****:** Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

8) ***Security threats*****:** The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

IV. MANETS CHARACTERISTICS

1) ***Distributed operation*****:** There is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

2) ***Multi hop routing*****:** When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) ***Autonomous terminal*****:** In MANET, each mobile node is an independent node, which could function as both a host and a router.

4) ***Dynamic topology*****:** Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

5) ***Light-weight terminals*****:** In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

6) ***Shared Physical Medium*****:** The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

V. GEOGRAPHICAL ROUTING PROTOCOLS

To decrease routing overhead, an approach that can be followed is to adopt location based routing. It provides with the location information of each node. Such location information helps in obtaining routing path which is precise and provides with the exact location of destination node, thus reducing routing overhead. Geographical protocols uses location information for traversing so these protocols calculate the position of each node using GPS (Global Positioning System) which require use of GPS satellite and GPS receiver for communication and the whole process works as follows:

A. GPS receiver communicates with GPS satellites for calculating its position.
B. Receiver receives the message via satellites.
C. Using those signals, position is then displayed in the form of latitude and longitude.

All the protocols that use geographical assistance for estimating node position are surveyed below and it is assumed that the nodes know their positions.

A. Geographical Addressing and Routing

Geographical addressing and routing allows message to be sent to all nodes in a specific geographical using geographical information instead of logical node addresses. A geographical destination addresses is expressed in three ways**: point**, **circle**(center point, radius), **polygon(point(l), paint(2), . . . , point(n-1)**,**point(n), point(l)**) where each vertex of the polygon is represented using geographic coordinates. This notation would be used to send a message to anyone within the specified geographical area defined by the closed polygon. For example, if we were to send a message to city hall in Fresno, California, we could send it by specifying the geographic limits of the city hall as a series of connected lines that form a closed polygon surrounding it. Therefore the address of the city hall in Fresno could look like: polygon([36.80,-119.801, 36,85,-119.761, . . .). A Geographical Router (GeoRouter) calculates its service area as the union of geographic area covered by the networks attached to it. This service area is approximated by a single closed polygon. GeoRouters exchange service area polygons to build routing tables. This approach builts hierarchical structure consisting of GeoRouters. The end users can move freely about the network. Data communication starts from a computer host capable of receiving and sending geographical messages (GeoHost), Data Packets are them sent to the local GeoNode(Residing in each subnet), which is responsible for forwarding the packets to the local GeoRouter. A GeoRouter first checks whether its service area intersects the destination polygon. As long as a part of the destination area is not covered, a GeoRouter sends a copy of the packet to its parent router for further routing beyond its own service area. Then its checks the service area of its child routers for possible intersection. All the child routers intersecting the target area are sent a copy of the packet.

When a router's service area falls within the target area, the router picks up a packet and forwards it to the GeoNodes attached to it. As GeoCast is designed for group reception, multicast group for receiving geographical messages are maintained at the GeoNodes. The incoming geographic messages are stored for a lifetime(determined by the sender) and during the time, they are multicast periodically through assigned multicast address. Clients at GeoHosts tune into the appropriate multicast address to receive the messages.

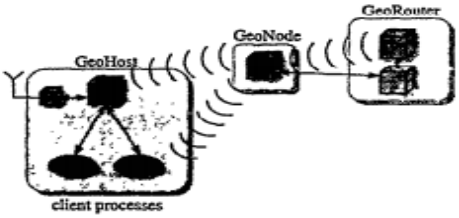
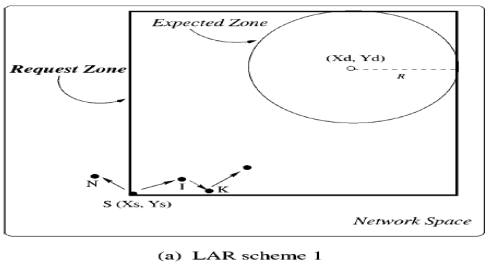


Fig 3: Components of the Geographic Routing System

B. **Location Aided Routing (LAR)**

The LAR protocol presented in is an on-demand protocol based on source routing. The protocol utilizes location information to limit the area for discovering a new route to a smaller request zone. As a consequence, the number of route request messages is reduced. The operation of LAR is similar to DSR. Using location information, LAR performs the route discovery through limited flooding (floods a request to a request zone). Only nodes in the request zone will forward route requests.. LAR provides two schemes to determine the request zone.

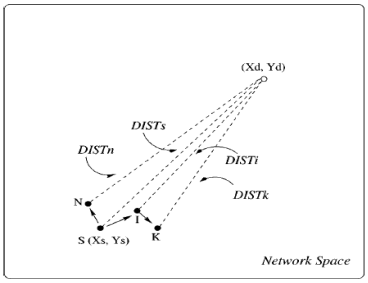
Scheme 1: The source estimates a circular area (expected zone) in which the destination is expected to be found at the current time. The position and size of the circle is calculated based on the knowledge of the previous destination location, the time instant associated with the previous location record, and the average moving speed of the destination. The smallest rectangular region that include the expected zone and the source is the request zone. The coordinates of the four corners of the zone are attached to route request by the source. During the route request flood, only nodes inside the request zone forward the request messages. As shown in fig. only nodes D,I,K are chosen for further forwarding as they lie within the request zone.



(a) LAR scheme 1

Fig 4: LAR Scheme 1

Scheme 2: The source calculates the distance to the destination based on the destination location known to it. This distance along with the destination location, is included in a route request message and sent to neighbors. When a node receives the request message only if its distance to the destination is less than or equal to the distance included in the request messages. For example, nodes and I will forward the requests from S as shown in fig 5. Before a node relays the request, it updates the distance field in the message with its own distance to the destination.



(b) LAR scheme 2

Fig 5: LAR Scheme 2

C. **Greedy Perimeter Stateless Routing**:

Uses the neighbor locaion information in forwarding data packets. Messages are periodically broadcast at each node to inform its neighbours of its position.Used Flooding technique. GPSR uses two forwarding strategy : Greedy Forwarding and perimeter forwarding.

Greedy Forwarding works this way: when a node receives a packet with the destination's location, it choses from its neighbors the node that is geographically closest to the destination and then forwards the data packet to it. This local optimal choice repeats at each intermediate node until the destination is reached. When a packet reaches a dead end (i.e. a node whose neighbours are all farther away from the destination than itself), perimeter forwarding is performed. Before performing the perimeter forwarding node needs to calculate a relative neighbourhood graph (RNG). Fig. shows the perimeter forwarding process, D is the destination node and X is the node position where the packet enters perimeter forwarding node. GPSR forwards it along the face intersected by the line XD. Packet forwarding is done using right-hand rule. In the worst case, GPSR will possibly generate a very long path before a loop detected.

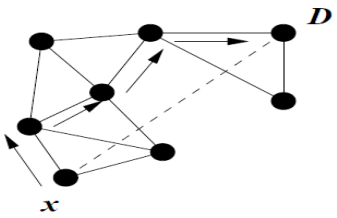


Fig 6: Perimeter Forwarding

D. **Location Area Based Adhoc Routing (LABAR**)

Routing protocol consist of two types of nodes namely: G-nodes and S-nodes. It is assumed that G-nodes know their positions precisely and S-node is assumed to have its position near to the position of G-node. Formation of virtual backbone is used for representing position of nodes, G-node(root) initiates virtual backbone formation and tracks the information using GPS which later on helps in directional routing over the network. Source G-node instructs node of its zone for how to forward packet inside the zone, Each zone node consults its G-node for best directionality instructions to forward packet to destination node.

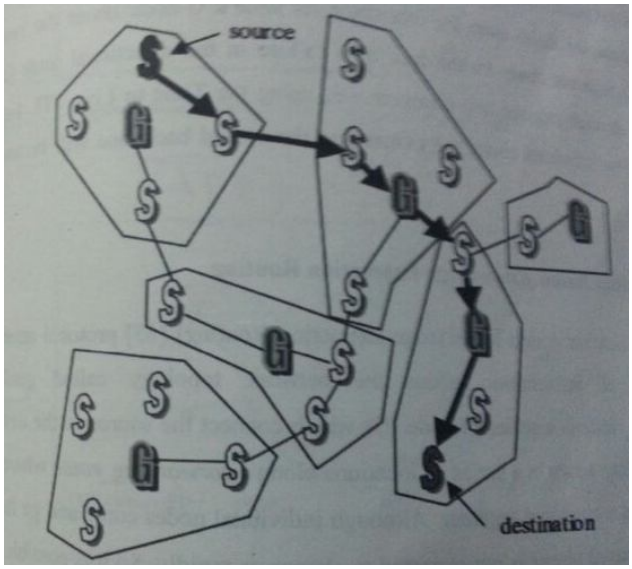


Fig 7: Route Process in LABAR

As shown in this figure, the source node queries the source G-node to map the destination IP address into the geographical location area of the destination. Then the source G-node determines the vector pointing from its own location to the destination's location. The resulting vectors direction is compared to each of the adjacent zone's direction and distance to determine which neighbouring zone should be used in relaying the data to the destination. After determining the next zone, the source G-node will instruct the source node(if different to the G-node) on how to route the packet inside the zone to reach the next zone with the least number of hops. Once a packet has left the source zone and entered in the source node query the source G-node node to map the destination IP address into the geographical location area of the destination. Then the source G-node determines the vector pointing from its own location to the destination's location. The resulting vectors direction is compared to each of the adjacent zones direction and distance to determine which neighbouring zone should be used in relaying the data to the destination. After determining the next zone, the source G-node will instruct the source node(if different from the G-node) on how to route the packet inside the zone to reach the next zone with the least number of hops.Once a packet has left the source zone and entered in intermediate zone, the node that receive the packet in the intermediate zone will be responsible to route the packet to the next intermediate (or final).Zone by consulting its Zone G-node about the best directionally matching adjacent zone.In case of a failure the directional route(determine e.g. through expired hop counter, i.e. using the time to live – TTL field) the source zone will be informed about the failure and the virtual backbone will be used to relay the packet.

E. **Location Aided Knowledge Extraction Routing (LAKER**)

LAKEER protocol attempts to cache a new kind of information about the network topology called guiding routes. A forwarding_route is a series of node ID's which connect the source to the destination hop by hop. A guiding_route is a series of locations along a forwarding_route where there seems to be many nodes clustered together. Although individual nodes come and go fast, the structure of these clustered places is not expected to change as rapidly. So it is possible to discover and cache this kind of guiding information during the route discovery process. Guiding_routes guide the route discovery direction more precisely and further narrow the search space even compared to the LAR approach. As example is illustrated in fig 7. P1 and P2 are two guiding positions along the guiding_route. The request zone of LAKER is defined by the location of the source node S, the guiding position and the "Expected zone", which is estimated region where the destination node is currently located.

LAKER requires zone helps in reducing routing overhead involved during transmission. Guiding_route also helps in finding void areas present over the network as shown in fig 8. if there is a void area (may be a lake) in a simulation area then the source node S has related guiding_route in cache, it can use the guiding information to direct the route discovery to pass around the void area without flooding the entire network.

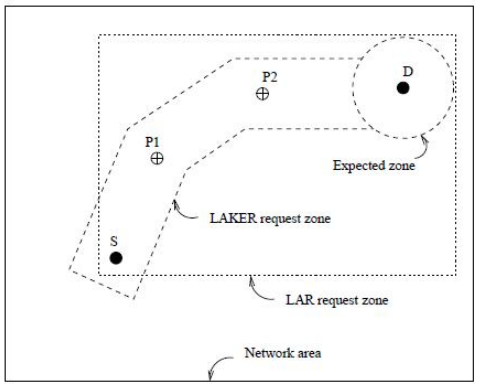


Fig 7: Comparing request zone of LAR and LAKER

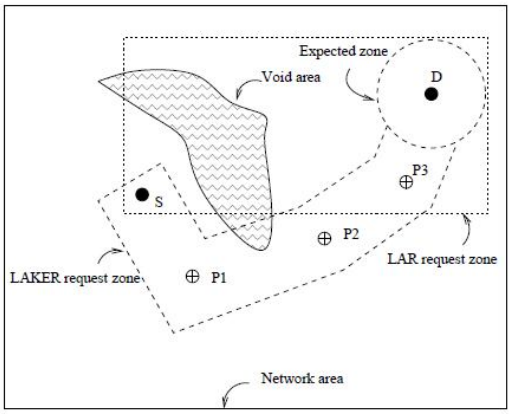


Fig 8: Route discovery in LAKER

VI. SUMMARY

This paper summarizes for how to make transmission of packet efficient in terms of routing and security. Routing can be made efficient by using GPS which provides location information of each node. Then geographica routing protocols such as LAR, LABAR, LAKER, GPSR are discussed which uses location information of each node for transmission of packets to the destination.

REFERENCES

[1] P. Agrawal, O. P.Vyas, P. Udaykumar," Analysis of MANET Security –Challenges, Threats & Solutions" International Journal Of Computer Science And Applications Vol. 3, No. 1, January / February 2010 ISSN: 0974-1003.

[2] Vikram m. Agrawal" Manet (Mobile Ad Hoc Network) – Challenges, Security And Protocols" International Journal of Computer science and Engineering Research and Development (IJCSERD),ISSN 2248- 9363

[3] Priyanka Goyal, Sahil Batra, Ajit Singh," A Literature Review of Security Attack in Mobile Ad-hocNetworks" International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010

[4] K. Thamizhmaran1, R. Santosh Kumar Mahto2, V. Sanjesh Kumar Tripathi3," Performance Analysis of Secure Routing Protocols in MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012

[5] Rachika Gupta," Mobile Adhoc Network(MANETS) :Proposed solution to Security Related Issues", Indian Journal of Computer Science and Engineering (IJCSE)

[6] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma," A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal Of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617

[7] Karan Singh, R. S. Yadav, Ranvijay," A Review Paper On Ad Hoc Network Security", International Journal of Computer Science and Security, Volume (1): Issue (1

[8] Amol Bhosle, Yogadhar Pandey ," Review of authentication and digital signature methods in Mobile ad hoc network **",** International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013

[9] Young-Bae Ko and Nitin H. Vaidya," Location-Aided Routing (LAR) in mobile ad hoc networks", Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA, 307–321,2000.

[10] Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", School of Information and Computer Science University of California, Irvine.

[11] Stefano B~agni, Irnrich Chlamtac, Violet R. Syrotiuk, Barry A. Woodward," A Distance Routing Effect Algorithm for Mobility", Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas.

[12] Brad Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Network", MobiCom 2000.

[13] Mohammed ERRITALI and Oussama Mohamed Reda and Bouabid El Ouahidi, "A Contribution To Secure The Routing Protocol "Greedy Perimeter Stateless Routing" Using A Symmetric Signature Based Aes And Md5 Hash" , International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.5, September 2011.

[14] Gergely V. Záruba, Vamsi K. Chaluvadi, and Azeem M. Suleman, "LABAR: Location Area Based Ad Hoc Routing for GPS-Scarce Wide-Area Ad Hoc Networks", Technical Report: CSE-2003-1.

[15] Jian Li and Prasant Mohapatra," LAKER: Location Aided Knowledge Extraction Routing for Mobile Ad Hoc Networks", Department of Computer Science, University of California, Davis, National Science Foundation through the grants CCR-0296070 and ANI-0296034.

[16] Manjuladevi.V, Jennie Bharathi.R, "MD5: Anonymous Location-Aided Routing in Suspicious Secure MANETs", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801.

[17] Aarti , Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks " , International Journal of Advanced Research in Computer Science and Software Engineering **,** Volume 3, Issue 5, May 2013 , ISSN: 2277 128X .

[18] Laura Marie Feeney, "A Taxanomy for Routing Protocols in Mobile Ad Hoc Networks", October 1999.

[19] Magnus Frodigh et. Al, "Wireless ad hoc networking- The art of networking without a network", Ericsson Review No. 4, 2000.

[20] Petteri Kuosmanen, "Classification of Ad Hoc Routing Protocol", January 2001.