International Journal of Computer Trends and Technology- volume4Issue2- 2013

Multicasting Over Manet Through Segmp By Secure Zone Leader Election

Bhavana.B.Turorikar[#], M.A.Shukla[*]

[#]*Master of computer Engineering (computer Network), Smt. KashibaiNavale college of engineering , PuneUniversity,Pune, India*

[*]*Department of computer Engineering, Smt. KashibaiNavale college of engineering, PuneUniversity, Pune, India*

***Abstract*— Now a day's group communications are important in Mobile Ad hoc Networks. Efficient method for implementing group communications is multicasting. But, due to difficulty in group membership management and multicast packet forwarding over a dynamic topology it is a challenge to implement efficient and scalable multicast with security in MANET. We propose a novel Secure Efficient Geographic Multicast Protocol (SEGMP) by modifying existing EGMP. SEGMP uses a virtual zone based structure to implement efficient and scalable group membership management scheme. In a broad terrain, a zone-based bi-directional tree is constructed to achieve more efficient membership management and multicast delivery of packets. To guide construction of zone structure, multicast tree construction and multicast packet forwarding, position information is utilized, which efficiently reduces the route overhead for route searching and tree structure maintenance. Many strategies have been further proposed to improve the efficiency of the protocol, by introducing the idea of zone depth used for building an optimal tree structure and integrating the location search of group members with the hierarchical group membership management. A scheme is also designed to handle empty zone problem faced by most routing protocols using a zone structure. Finally, we design a scheme to elect a zone leader through voting and handle security of votes using ECDSA algorithm for multicasting over MANETS in a virtual zone based network. The scalability and the efficiency of SEGMP are evaluated through simulations and quantitative analysis. Our results demonstrate that SEGMP has high packet delivery ratio, and low energy consumption and multicast group joining delay under all test scenarios, and is also scalable to both group size and network size. Compared to Efficient Geographic Multicast Protocol (EGMP), SEGMP has significantly high packet delivery ratio, less energy consumption and multicast group joining delay.**

***Keywords*— Geographic Routing, Mobile Ad Hoc Networks, Multicasting, Protocol, Wireless Networks.**

I. INTRODUCTION

Ad-Hoc Networks also called as Mobile Ad-Hoc Network (MANET) is a group of wireless mobility nodes which organizes itself in a network without the need of any infrastructure. There are increasing interests and importance in supporting group communication over Mobile Ad Hoc Networks (MANETs) [1]. It is a big challenge in developing a robust multicast routing protocol for dynamic Mobile Ad-Hoc Network (MANET).

MANETs are used in many critical areas such as disaster relief efforts, emergency warnings in vehicular networks, supports for multimedia games and video conferencing and many more. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile Environment. Multicast is the delivery of a message or Information to a group of destinations simultaneously in a single transmission using routers, only when the topology of the network requires it. Multicasting is an efficient method to realize group communications with a one-to-many or many-to-many relationship transmission pattern. However, there is a big challenge in enabling efficient multicasting over a MANET whose topology may change constantly.

In this work, we propose a Secure Efficient Geographic Multicast Protocol, SEGMP, which can extend to a large group size and large network size. This protocol is actually designed to be comprehensive and self-contained, but simple and efficient for more reliable operation and high packet delivery ratio, less energy consumption and multicast group joining delay when compared to existing one. Instead of addressing only a specific part of the problem, it considers a zone-based scheme to efficiently handle membership management of the group, and takes advantage of the membership management structure to efficiently track the locations of all the group members without resorting to an external location server. The structure of zone is formed virtually and the zone where a node is located can be calculated based on the position of the node and a reference origin. A conventional topology-based multicast protocol can be described in two categories, tree-base and mesh-based protocols. The tree-based protocols construct a tree structure for more efficient forwarding of packets to all the group members. In Mesh-based protocols multicast tree with additional paths can be used to forward packets in case on any link failure.

In topology based cluster model, a cluster is normally formed around a cluster leader with nodes which are one hop or k-hop away, and as network topology changes the cluster will constantly change. But there is no need to include a big overhead to create and maintain the geographic zones proposed in this work of cluster model, which is critical to support more efficient and reliable communications over a dynamic MANET. In a zone based network structure, since network terrain is divided into square zones a zLdr(zone leader) is elected in each zone for managing the local zone group membership and taking part in the upper tier multicast routing. Now, in the existing protocol the node which is closer to the centre is elected as the zone leader but in proposed protocol the zone leader is elected through secured election process which is carried among the members of the same zone members.

II. RELATED WORK

Multicasting in mobile ad hoc networks is a relatively unexplored research area, when compared to the area of unicast routing for MANET. Many applications visional for mobile ad-hoc networks rely on group communication. As a consequence, multicast routing in mobile ad-hoc networks has attracted significant attention over the recent years.

Geographic routing protocols [12] are generally more scalable and reliable than conventional topology-based routing protocols [1] [4] with their forwarding decisions based on the local topology. In MANET, geographic routing protocols unicast routing [8], [12], [13] have been proposed in recent years for more scalable and robust packet transmissions. In the existing position based geographic routing protocols it is generally assume that mobile nodes are aware of their own positions through certain positioning system like Global Positioning system (GPS), and a source can obtain the destination position through some type of location service [18] [22]. In GPSR [12], the intermediate node makes its forwarding choices based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic change of the neighbors. Similarly in SPBM [17], the packets form the source with the header are forwarded are based on the next hop position. In order to extend position-based unicast to multicast routing, SPBM provides an algorithm for duplicating multicast packets at intermediate nodes if destinations for that packet are no longer located in the same direction.

Similarly, to reduce the overhead of topology maintenance for dynamic MANET and support more reliable multicasting, an alternative is to make use of the position information to guide multicast routing. However, many challenges are there in implementing an efficient and robust geographic multicast scheme in MANET. A direct way to extend the geography-based transmission from unicast to multicast is to put the addresses and positions of all the members into the packet header, but, the header overhead will increase significantly as the group size increase, which constrains the application of geographic multicasting only to a small group.

Topology-Based Multicast Routing Protocols [17]:

Topology-based multicast protocols for mobile ad-hoc networks can be categorized into two main classes: tree-based and mesh-based protocols. In a tree-based approach data dissemination tree is build that contains exactly one path from a source to each destination. The topological information is used for its construction. Trees can be sub-classified further into source trees and shared trees. The topology-based multicast protocols are generally difficult to scale to a large network size, since the construction and maintenance of the conventional tree or mesh structure involve high control overhead over a dynamic network.

Position-Based Unicast and Multicast Routing Protocols [17]:

The forwarding decisions in position-based routing are usually based on the node's own position, position of destination, and position of the node's direct radio neighbors. As there is no global distribution structure such as a route is required, position-based routing is considered to be very robust to mobility. It actually performs best when the next-hop node can be found in a greedy manner by simply minimizing the remaining distance to the destination. However, there are some situations where this strategy leads to a local optimum, and no neighbor can be found greedily to forward the packet further, although a route exists. [17] Deals with the "Location-Guided Tree Construction Algorithms", where the sender includes the addresses of all destinations in the header of a multicast packet. Additional to this, the location of all destinations is included as well. It remains open how the sender is able to obtain the position information, and the scaling limitations.

Location-Based Multicast Protocols [22]:

Two approaches may be used to implement location based Multicast: First, maintain a multicast tree, all nodes within multicast region at any time belong to the multicast tree. The tree would need to be updated whenever nodes enter or leave the multicast region. Second, do not maintain a multicast tree. In this case, the multicast may be performed using some sort of "flooding" scheme. This paper considers multicast group members send a packet to specific multicast region.

III. EXISTING PROTOCOL AND ITS PERFORMANCE

A) Protocol Overview

The main goal of EGMP is to supports scalable and reliable membership management and multicast forwarding through a two-tier virtual zone- based structure. At the lower layer, with reference to a predetermined virtual origin, the nodes in the network self organize themselves into a set of zones, and to manage the local group membership a leader is elected in a zone ie. *zLdr*. At the upper layer, the leader serves as a representative for its zone to join or leave a multicast group as an when required. This results in construction of a network-wide zone-based multicast tree is. To provide efficient and reliable transmissions and management, location information will be integrated with the design and used to guide the zone construction, multicast tree construction and maintenance, packet forwarding and group membership management. The zone-based tree is shared among all the multicast sources of a group.

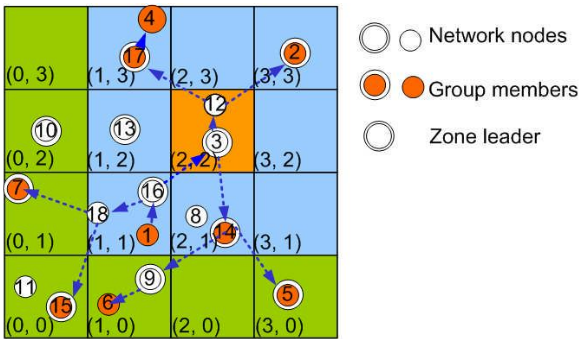

Fig 1: Zone structure and multicast session example

Some of the notations to be used are:

- *zone:* The network terrain is divided into square zones as shown in Fig. 1.
- *r:* Zone size, the length of a side of the zone square. The zone size is set to r <= rt/sqrt(2), where rt is the transmission range of the mobile nodes.
- *zone ID:* The identification of a zone. A node can calculate its zone ID (a, b) from its position coordinates(x,y) as:$a=[(x-x_0)/r],b=[(y-y_0)/r]$ where (x0; y0) is the position of the virtual origin, which is known reference location or can be determined at network setup time. A zone is virtual and calculated in reference to the virtual origin. For easy understanding, we assume the entire zone IDs is positive.
- *zone center:* For a zone with ID (a,b), the position of its center (xc; yc) can be calculated as: $xc=x0+(a+0.5)*r$, $yc=y0+(b+0.5)*r$. A packet destined to a zone will be forwarded toward the center of the zone.
- *zLdr:* Zone leader. A zLdr is elected in each zone for managing the local zone group membership and taking part in the upper tier multicast routing.
- *tree zone:* The tree zones are responsible for the multicast packet forwarding. It may have group members or will just help to forward the multicast packets for zones with members.
- *root zone:* It is the zone where the root of the multicast tree is located.
- *zone depth:* To reflect its distance to the root zone the depth of a zone is used

In EGMP, the zone structure is virtual and calculated based on a reference point. Hence, the zone structure construction does not depend on the shape of the network region, and it is very simple to locate and maintain a zone. To provide location reference and support lower-level group membership management the zone is used in EGMP. A multicast group can cross multiple zones. As EGMP is introduced with virtual zone, it does not need to track individual node movement but only needs to track the membership change of zones; this significantly reduces the management overhead and increases the robustness of the proposed multicast protocol.

D) Multicast Route Maintenance and Optimization

In a dynamic network, it is critical to maintain the multicast tree connection, and adjust the tree structure upon the topology changes to optimize the multicast routing. Due to the movement of nodes between different zones, some zones may become empty in the zone structure, it becomes critical to handle empty zone problem in a zone-based protocol. As compared to manage the connections of individual nodes, there is a much lower rate of zone membership change and hence a much lower overhead in maintaining the zone-based tree. A disconnected zone can quickly reestablish its connection to the tree as the tree construction is guided by location information. In addition, a zone may be partitioned into multiple clusters due to fading and signal blocking.

IV SECURE EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL (SEGMP)

In SEGMP, the zone structure is virtual and calculated based on a reference point. The zone structure construction does not depend on the shape of the network region and hence it becomes easy to locate and maintain a zone. The zone is used in SEGMP to support lower-level group membership management and provide location reference. A multicast group can cross multiple zones. With the introduction of virtual zone, SEGMP does not need to track individual node movement but only needs to track the membership change of zones, which significantly increases the robustness and reduces the management overhead of the proposed multicast protocol.

A) Neighbor Table Generation and Zone Leader Election

A node constructs its neighbor table without need of extra signaling. After receiving a beacon from a neighbor, a node records the node ID, flag and position, contained in the message in its neighbor table. The zone ID of the sending node can be calculated from its position. To avoid routing failure due to outdated topology information, if not refreshed within a period *TimeoutNT* an entry will be removed or the corresponding neighbor is detected unreachable by the MAC layer protocol.

For efficient management of states in a zone, a leader with minimum overhead is elected. A zone leader is elected through the cooperation of nodes and maintained consistently in a zone. In a network when a node appears, it existence is announced by sending out a beacon. Then, it waits for an Intval_{max} period for the beacons from other nodes. Every Intval_{min} a node will check its neighbor table and determine its zone leader under different cases: 1) the neighbor table contains no other nodes in the same zone; it will announce itself as the leader. 2) Flags of all the nodes in the same zone are unset, which indicates that no node in the zone has announced the leadership role. The zone leader is elected through secure election process. Here each node sends as vote message to its neighbouring nodes. Each receiving node stores this vote info in vote list then each node sends vote announcement to its neighbour it contains (Zone ID, No of votes, Signature --(Generate Signature in each node)). While receiving this announcement receiving node verifies its signature with receiving one. If it does not match then discard the announcement but if it is matches include neighbour vote list. Then check highest vote receiving node and the node with highest votes is selected and that node acts as a Zone leader. 3) Only one of the nodes in the zone has its flag set, and then the node with the flag set is the leader.

Elliptic Curve Digital Signature Algorithm (ECDSA) [23]

The security of the voting process is carried by the ECDSA algorithm. The elliptic curve discrete logarithm problem is the cornerstone of much of present-day elliptic curve cryptography. ECDSA relies on the natural group law on a non-singular elliptic curve which allows one to add points on the curve together. For a givenn elliptic curve *E* a point on that curve, *P*, over a finite field F, and another point you know to be an integer multiple of that point *Q*, the problem is to find integer *n* such that $nP = Q$.

The problem is computationally difficult unless the curve has a “bad” number of points over the given field, where “bad” consists of various collections of numbers of points which make the elliptic curve discrete algorithm problem breakable. Let’s take an example, if the number of points on *E* over F is the same as the number of elements of F, then the curve is vulnerable to attack .Due of these issues that point-counting on elliptic curves is such a hot topic in elliptic curve cryptography.

Elliptic Curve DSA (ECDSA)

This part describes the procedures for generating and verifying signatures using the ECDSA.

A) DOMAIN PARAMETER GENERATION

For ECDSA the domain parameter consist of a suitably chosen elliptic curve *E* defined over a finite field F*p* of characteristic *p* and a base point $G \in Ep(a,b)$ with order *n*.

1. Select a random integer or pseudo-random integer *x* such that $1 \le x \le n-1$.
2. Compute $Q = xG$.
3. A’s public key is *Q* and A’s private key is *x*.

B) ECDSA SIGNATURE GENERATION

To sign a message *m*, an entity A with domain parameters $(p,Ep(a,b),G,n)$ and associated key pair (x,Q) does the following:

1. Select an integer *k* such that $1 \le k \le n-1$.

2. Compute $kQ = (x1,y1)$.
3. Compute $r = x1 \pmod n$. If $r = 0$ then go to step 1.
4. Compute $k{-1} \pmod n$.
5. Compute SHA-1(m) and then convert this string to an integer $H(m)$.
6. Compute $s = k{-1}(H(m)+xr) \pmod n$. If $s = 0$, then go to step 1.
7. A's signature for message m is (r, s).

C) ECDSA SIGNATURE VERIFICATION

To verify A's signature (r, s) on m, B obtains an authentic copy of A's domain parameter $(p,Ep(a,b),G,n)$ and associated public key Q. Then B does the following:

1. Verify that whether r and s are integers in the interval $[1,n{-1}]$.
2. Compute SHA-1(m) and then convert this string to an integer $H(m)$.
3. Compute $w = s{-1} \pmod n$.
4. Compute $u1 = H(m)w \pmod n$ and $u2 = rw \pmod n$.
5. Compute $X = (x2,y2) = u1G+u2Q$.
6. If $X = O$, then reject the signature. Otherwise, compute $v = x2 \pmod n$.
7. Accept the signature if and only if $v = r$.

D) PROOF THAT SIGNATURE VERIFICATION WORKS

If a signature (r, s) on a message m was indeed generated by A, then $s = k{-1}(H(m)+xr) \pmod n$. Rearranging gives

$$\begin{aligned} kG &= s{-1}(H(m)+xr)G \pmod n \\ &= s{-1}H(m)G+s{-1}rxG \pmod n \\ &= H(m)wG+rwQ \pmod n \\ &= u1G+u2Q \pmod n. \end{aligned}$$

Thus $u1G+u2Q = (u1+u2d)G = kG$, and so $v = r$ as required.

V RESULTS AND DISCUSSIONS

We focus on the studies of the scalability and efficiency of the protocol under the dynamic environment and also in consideration with the energy and power utilization of nodes. The performance of the proposed SEGMP algorithm is evaluated via NS2 simulator. Performance metrics are utilized in the simulations for performance comparison

A) Simulation Tool

This paper uses the simulation tool NS2 for analysis which is highly preferred by research communities.

NS is a discrete event simulator targeted at networking research. It also provides substantial support for simulation of routing, TCP, and multicast protocols over wired and wireless (local and satellite) networks. NS2 is an object oriented simulator, which is written in C++, with frontend as an OTcl interpreter. This means that most of the simulation scripts are created in Tcl(Tool Command Language). Both tcl and C++ have to be used if the components have to be developed for ns2.

B) Simulation Setup

The performance analysis is done on Linux – red hat 9.0 Operating System. Ns –allinone-2.29 was installed on the platform using tool Vm ware Work station .Simulation time is 200s .Number of nodes is 100,125,150,175,200.Traffice is CBR(constant Bit rate).CBR packet size 1400 bytes. Simulation area size 700*700m

C) Performance Metrics Used

For the analysis of EGMP and MSEGMP routing protocols following metrics are used in this paper

i) Packet Delivery Ratio
ii) Average End to End Delay
iii) Throughout

Packet delivery ratio: Packet delivery ratio is defined as the ratio between the number of packets sent by constant bit rate sources (CBR, "application layer") and the number of received packets by the CBR sink at destination
.

Routing Overhead: It is the number of packet generated by routing protocol during the simulation. Where overhead is the control packet number generated by node i. Generation of an important overhead will decrease the protocol performance.

Average end-to-end delay of data packets: Average time is the time elapsed for delivering a data packet within a successful transmission

Energy consumption: Energy consumption is for the entire network, including transmission energy consumption for both the data and control packets.

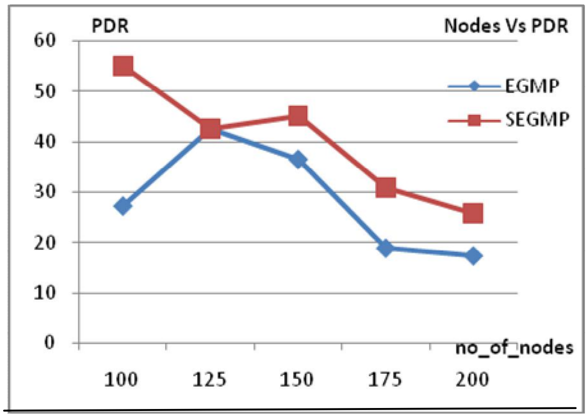

Fig 2. Comparison of PDR between EGMP and SEGMP

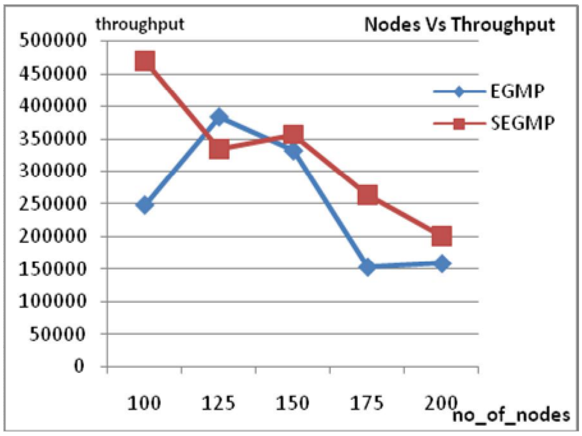

Fig 3 Comparison of throughput between EGMP and SEGMP

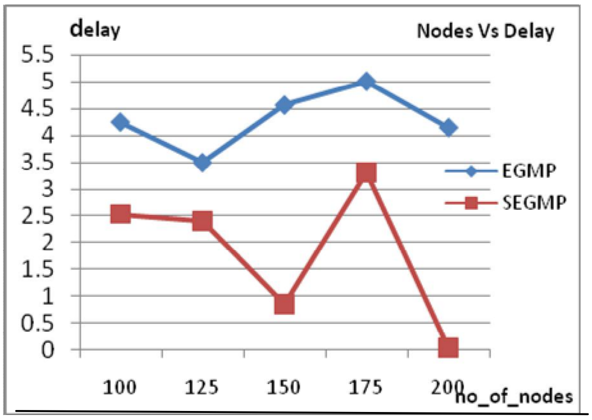

Fig 4 Comparison of End-to-End delay between EGMP and SEGMP

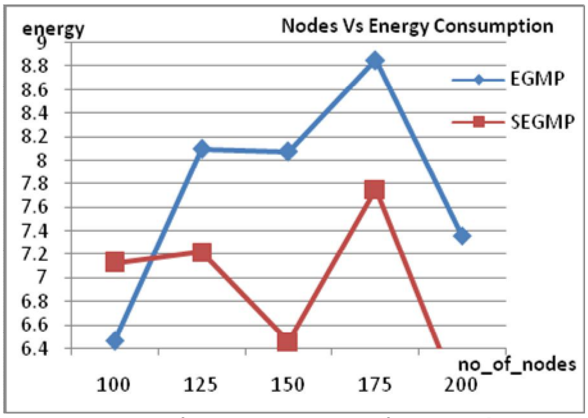

Fig 5 Comparison of Energy consumption of EGMP with SEGMP

VI. CONCLUSIONS

There is an increasing demand and a big challenge to design more scalable and reliable multicast protocol over a dynamic ad hoc network (MANET). In this paper, we proposed secure efficient and scalable geographic multicast protocol, SEGMP, for MANET. The scalability of EGMP is achieved through a two-tier virtual-zone-based structure which takes advantage of the geometric information to greatly simplify the zone management and packet forwarding. A zone-based bidirectional multicast tree is built at the upper tier for more efficient multicast membership management and data delivery, at the lower tier to realize the local membership management the intra zone management is performed. The position information is used in the protocol to guide the zone structure building, maintenance, multicast tree construction and multicast packet forwarding. As compared to conventional topology-based multicast protocols, use of location information in EGMP significantly reduces the tree construction and maintenance overhead and also enables quicker tree structure adaptation to the network topology change. To handle the empty zone problem we also develop a scheme, which is challenging for the zone-based protocols. Additionally, SEGMP makes use of secured voting process for election of zone leaders by using secured ECDSA algorithm.

Compared to ODMRP a classical protocol, both geometric multicast protocols SPBM and EGMP could achieve much higher delivery ratio in all circumstances, with respect to the variation of mobility, node density, group size, and network range.

Our results indicate that for efficient management of states in zone, a zone leader with minimum overhead is elected. A zone leader is elected through secured voting process and handling of votes among the nodes in the same zone is done using a secure algorithm ECDSA. The node with the highest number of votes i.e. the node with highest number of neighbours is elected as zone leader .Our simulation results demonstrate that SEGMP has low energy consumption, high packet delivery ratio, and high throughput and low multicast group joining delay under all cases studied, and is scalable to both the group size and the network size. Compared to the geographic multicast protocol SPBM and EGMP, it has significantly lower control overhead, multicast group joining delay and data transmission overhead.

ACKNOWLEDGMENT

I would like to thank **Prof. Mrs. M.A. Shukla** for helping me out in selecting the topic and contents, giving valuable suggestions in preparation of paper. Thanks to all the colleagues for their extended support and valuable guidance.

Last but not least my dear family who supported me very well by taking care of all my responsibilities. I am grateful for it and would like to give sincere thanks to my family for all.

REFERENCES

[1] X. Xiang and X. Wang, "An Efficient Geographic Multicast Protocol for Mobile Ad Hoc Networks," Proc. IEEE Int'l Symp. World of Wireless,Mobile and Multimedia Networks (WoWMoM), June 2006.

[2] E.M. Royer and C.E. Perkins, "Multicast Operation of the Ad Hoc On-Demand Distance Vector Routin Protocol," Proc. ACM /IEEE MobiCom, pp. 207-218, Aug. 1999.

[3] X. Zhang and L. Jacob, "Multicast Zone Routing Protocol in Mobile Ad Hoc Wireless Networks," Proc Local Computer Networks (LCN '03), Oct. 2003.

[4] C.Wu, Y.Tay, and C.K. Toh, "Ad Hoc Multicast Routing Protocol Utilizing Increasing Id-Number (AMRIS) Functional Specification," Internet draft, Nov. 1998.

[5] S. Wu and K.S. Candan, "GMP: Distributed Geographic Multicast Routing in Wireless Sensor Networks," Proc 26th IEEE Int'l Conf. DistributedComputing System(ICDCS '06), 2006.

[6] S.M. Das, H. Pucha, and Y.C. Hu, "Distributed Hashin for Scalable Multicast in Wireless Ad Hoc Network,"IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 3, pp. 347-362, Mar. 2008.

[7] C. Gui and P. Mohapatra, "Scalable Multicasting For Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, Mar. 2004.

[8] X. Xiang, Z. Zhou, and X. Wang, "Self-Adaptive On Demand Geographic Routing Protocols for Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, May 2007.

[9] M. Mauve, H. Fubler, J. Widmer, and T. Lang,"Position-Based Multicast Routing for Mobile Ad-Hoc Networks," Proc.ACM MobiHoc, poster section, June 2003.

[10] M. Gerla, S.J. Lee, and W. Su, "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks," Internet draft, draftietf- manet- odmrp-02, 2000.

[11]H.Vijayakumar, M.Ravichandran "Efficient Location Management of Mobile Node in Wireless Mobile Ad- hoc Network" Proceedings of the National Conference on Innovations in Emerging Technology 2011.

[12] B. Karp and H.T. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM/IEEE MobiCom, pp. 243-254, Aug. 2000.

[13] Shuhui Yang, Jie Wu "New Technologies of Multicasting In Manet".

[14] Chatchai Khunboa and Robert Simon "Mobile Ad Hoc Multicasting to Support Distribute Virtual Environments" IEEE Transactions-2004.

[15] T. Camp and Y. Liu, "An Adaptive Mesh-Based Protocol for Geocast Routing," J. Parallel an Distributed Computing, vol. 63, no. 2, pp. 196-213,2003.

[16] Manik Kapil "Security Issues In Mobile Ad Hoc Networks".

[17] M. Transier, H. Fubler, J. Widmer, M. Mauve, and W.Effelsberg, "A Hierarchical Approach to Position Based Multicast for Mobile Ad-Hoc Networks," Wireless Networks, vol. 13, no. 4, pp. 447-460, Aug2007.

[18] J. Li et al., "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM/IEEE MobiCom, pp. 120-130, 2000.

[19] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad-hoc wireless networks," Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, pp. 153–81, 1996.

[20] Juan A. Sanchez, Pedro M. Ruiz, Ivan Stojmenovic "GMR: Geographic Multicast Routing for Wireless Sensor Networks" IEEE Communications Society 2006.

[21] Young-Bae Ko and Nitin H. Vaidya "Geocasting in Mobile Ad Hoc Networks: Location-Based Multicast Algorithms'

[22] S. Giordano and M. Hamdi, "Mobility Management:The Virtual Home Region," technical report, Oct. 1999.

[23] **"**Modified Efficient Geographic Multicast Protocol in Multicasting over Mobile Ad HocNetworks for QOS Improvements" M.Subha, M.Manoranjani, Journal of Computer Applications (JCA)ISSN: 0974-1925, Volume IV, Issue 2, 2011

[24] "On the Elliptic Curve Digital Signature Algorithm" Hung-Zih Liao , Yuan-Yuan Shen, July 2006

Mrs Bhavana.B.Turorikar pursuing her ME (Computer Networks) from Pune University. She has 3 yrs in teaching experience. Her area of interest is Mobile Computing and Network Security.

Mrs M.A. Shukla, ME(E&TC). She has experience above 25yrs as Head of Department of Computer Engineering. Her area of interest is Parallel Computing and Wireless Communications network