

# Performance Evolution of Scalable Multicasting Over Mobile Ad-Hoc Networks

<sup>1</sup>Dr. K. Ramakrishnaiah, <sup>2</sup>P. Prathibha, <sup>3</sup>D. Hari Krishna

<sup>1,2,3</sup>Dept. of CSE, NOVA College of Engineering & Technology, Vijayawada, AP, India

## Abstract

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 propose an efficient and scalable geographic multicast protocol, EGMP, 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 bi-directional multicast tree is built at the upper tier for more efficient multicast membership management and data delivery, while the intra-zone management is performed at the lower tier to realize the local membership management. The position information is used in the protocol to guide the zone structure building, multicast tree construction, maintenance, and multicast packet forwarding. Compared to conventional topology based multicast protocols, the use of location information in EGMP significantly reduces the tree construction and maintenance overhead, and enables quicker tree structure adaptation to the network topology change. We also develop a scheme to handle the empty zone problem, which is challenging for the zone-based protocols. Additionally, EGMP makes use of geographic forwarding for reliable packet transmissions, and efficiently tracks the positions of multicast group members without resorting to an external location server. We make a quantitative analysis on the control overhead of the proposed EGMP protocol and our results indicate that the per-node cost of EGMP keeps relatively constant with respect to the network size and the group size. We also performed extensive simulations to evaluate the performance of EGMP. Compared to the classical protocol ODMRP, 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. However, compared to EGMP, SPBM incurs several times of control overhead, redundant packet transmissions and multicast group joining delay. Although SPBM is designed to be scalable to the group size, it has very low packet delivery ratio when the group size is small without a stable membership in each level of quad-tree square, and cannot perform well under a large network size due to the use of multi-level network-wide flooding of control messages. ODMRP takes advantage of broadcasting to achieve more efficient packet forwarding, but the transmissions are much more unreliable due to its difficulty of maintaining forwarding mesh under mobility, which leads to a lower packet delivery ratio. The multicast group joining delay of ODMRP is also much higher than that of EGMP. Our results indicate that geometric information can be used to more efficiently construct and maintain multicast structure, and to achieve more scalable and reliable multicast transmissions in the presence of constant topology change of MANET. Our simulation results demonstrate that EGMP has high packet delivery ratio, and low control overhead and 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, it has significantly lower control overhead, data transmission overhead, and multicast group joining delay.

## Keywords

Multicasting, Mobile Ad-Hoc Networks, EGMP, SPBM

## I. Introduction

The provision of security services in the MANET context faces a set of challenges specific to this new technology. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified [4-5], in literature as such challenges. Nevertheless, the single most important feature that differentiates MANET is the absence of a fixed infrastructure. No part of the network is dedicated to support individually any specific network functionality, with routing (topology discovery, data forwarding) being the most prominent example. Additional examples of functions that cannot rely on a central service, and which are also of high relevance to this work, are naming services, Certification Authorities (CA), directory and other administrative services. Even if such services were assumed, their availability would not be guaranteed, either due to the dynamically changing topology that could easily result in a partitioned network, or due to congested links close to the node acting as a server. Furthermore, performance issues such as delay constraints on acquiring responses from the assumed infrastructure would pose an additional challenge. The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them. In the MANET context, there may be no ground for an a priori classification, since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Additionally, in MANET freely roaming nodes form transient associations with their neighbors, join and leave MANET sub-domains independently and without notice. Thus it may be difficult in most cases to have a clear picture of the Ad-Hoc network membership. Consequently, especially in the case of a large-size network, no form of established trust relationships among the majority of nodes could be assumed. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The mechanisms currently incorporated in MANET routing protocols cannot cope with disruptions due to malicious behavior. For example, any node could claim that is one hop away from the sought destination, causing all routes to the destination to pass through itself. Alternatively, a malicious node could corrupt any in-transit route request (reply) packet and cause data to be misrouted. The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, and, as a result, the network nodes would have to rely on cycles of time-out and new route discoveries to communicate. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. In particular,

intentionally falsified routing messages would result in a Denial-of-Service (DoS) experienced by the end nodes. The proposed here scheme combats such types of misbehavior and safeguards the acquisition of topological information. Our scheme guarantees that a node initiating a route discovery will be able to identify and discard replies providing false topological information, or, avoid receiving them. Our protocol departs from the Internet related solutions [2], which require the existence of a trust structure that encompasses all nodes participating in routing, and may rely on network management operations to detect routing instabilities. Moreover, the novelty of our scheme, as compared with other MANET secure routing schemes, is that false route replies, as a result of malicious node behavior, are discarded partially by benign nodes while in-transit towards the querying node, or deemed invalid upon reception. Most importantly, the above-mentioned goals are achieved with the existence of a security association between the pair of end nodes only, without the need for intermediate nodes to cryptographically validate control traffic. The widely accepted technique in the MANET context of route discovery based on broadcasting query packets is the basis of our protocol. More specifically, as query packets traverse the network, the relaying intermediate nodes append their identifier (e.g., IP address) in the query packet header. When one or more queries arrive at the sought destination, replies that contain the accumulated routes are returned to the querying node; the source then may use one or more of these routes to forward its data. Reliance on this basic route query broadcasting mechanism allows our proposed here Secure Routing Protocol (SRP) to be applied as an extension of a multitude of existing routing protocols. In particular, the Dynamic Source Routing (DSR) [8] and the IERP [13], of the Zone Routing Protocol (ZRP) [14], framework are two protocols that can be extended in a natural way to incorporate SRP. Furthermore, other protocols such as ABR, for example, could be combined with SRP with minimal modifications to achieve the security goals of the SRP protocol. SRP guarantees the acquisition of correct topological information in a timely manner, i.e., the route replies that are validated and accepted by the querying node provide accurate connectivity information, despite the presence of strong adversaries. The protocol is proven robust against a set of attacks that attempt to compromise the route discovery, under the assumption of non-colluding adversarial nodes. In the sequel, we review schemes related to the problem at hand and then present our scheme. First, a concise overview is provided, followed by the detailed definition in section D. The analysis of the protocol is given next, with a discussion of related issues in section F.

## II. Existing System

In this section, we first summarize the basic procedures assumed in conventional multicast protocols, and then introduce a few geographic multicast algorithms proposed in the literature. Conventional topology-based multicast protocols include tree-based protocols (e.g., [3-5]) and mesh-based protocols (e.g., [6,8]). Tree-based protocols construct a tree structure for more efficient forwarding of packets to all the group members. Mesh-based protocols expand a multicast tree with additional paths which can be used to forward packets when some of the links break. Although efforts were made to develop more scalable topology-aware protocols [7], the topology-based multicast protocols are generally difficult to scale to a large network size, as the construction and maintenance of the conventional tree or mesh structure involve high control overhead over a dynamic network. The work in attempts to improve the stateless multicast

protocol [2], which allows it a better scalability to group size. In contrast, EGMP uses a location-aware approach for more reliable membership management and packet transmissions, and supports scalability for both group size and network size. As the focus of our paper is to improve the scalability of location-based multicast, a comparison with topology-based protocols is out of the scope of this work. However, we note that at the similar mobility and system set-up, the delivery ratio is much lower than that of EGMP, and the delivery ratio in varies significantly as the group size changes. In addition, topology-based routing by nature is more vulnerable to mobility and long path transmission, which prevents topology-based protocols from scaling to a large network size. Besides the need of managing group membership as well as constructing and maintaining a multicast structure, a geographic multicast protocol also requires a location service to obtain the positions of the members. The geographic multicast protocols presented need to put the information of the entire tree or all the destinations into packet headers, which would create a big header overhead

when the group size is large and constrain these protocols to be used only for small groups. In DSM, each node floods its location in the network. A source constructs a Steiner tree and encodes the multicast tree into each packet, and delivers the packet by using source routing. LGT requires each group member to know the locations of all other group members, and proposes two overlay multicast trees: a bandwidth-minimizing LGS tree and a delay-minimizing LGK tree. In PBM, a multicast source node finds a set of neighboring, next-hop nodes and assigns each packet destination to one next-hop node. The next-hop nodes, in turn, repeat the process. Thus, no global distribution structure is necessary. GMP attempts to build a more efficient multicast tree through a centralized calculation for tree construction, and is also more applicable for a smaller group. The focus of EGMP, however, is to improve the scalability and efficiency of geometric multicast. The HRPM and SPBM are more related to our work, as they also support hierarchical group management. HRPM consists of two key design ideas: 1) hierarchical decomposition of a large group into a hierarchy of recursively organized manageable-sized subgroups and 2) the use of distributed geographic hashing to construct and maintain such a hierarchy. Although it is interesting to apply hashing to find the Rendezvous Point (RP) for the network to store and retrieve state information, the hashed location is obtained with the assumption of the network size, which is difficult for a dynamic network. Also, as the hashed location is virtual, it is possible that the nodes could not find the (consistent) RP. This can happen when a message (e.g., Join) reaches a node whose transmission range covers the virtual point, but the node is neither the one closest to the RP, nor aware of the node (which may be out of its transmission range) closest to the RP. The mobility of nodes will introduce additional challenge to the protocol, which may not only result in frequent RP handoff, but also increase the chance of RP search inconsistency and failure. Additionally, requiring a node to contact RP first for a Join will increase joining delay. In contrast, EGMP does not make any assumption of the network size in advance, and the change of the membership of a zone does not need to be sent to a far-away RP but only needs to be updated locally. Instead of using one RP as a core for group membership management, which may lead to a point of failure, EGMP introduces the root zone which is much more stable than a single point, and manages group membership more efficiently within the local range. Instead of using the overlay-based multiple unicast transmissions, EGMP takes advantage of

the promiscuous mode transmission to forward packets along more efficient transmission paths. We did not directly compare our work with HRPM, as we do not know the hashing algorithm used and a different RP distribution scheme would lead to different performance. However, we evaluated the performance of EGMP using a much larger default network size, which is known to have much more challenge to ensure reliable multicast transmissions than a smaller network. In SPBM, the network terrain is divided into a quadtree with  $L$  levels. The top level is the whole network and the bottom level is constructed by basic squares. Each higher level is constructed by larger squares with each square covering four smaller squares at the next lower level. All the nodes in a basic square are within each other's transmission range. At each level, every square needs to periodically flood its membership into its upper level square. Such periodic flooding is repeated for every two neighboring levels and the top level is the whole network region. Significant control overhead will be generated when the network size increases as a result of membership flooding. With this proactive and periodic membership updating scheme, the membership change of a node may need to go through  $L$  levels to make it known to the whole network, which leads to a long multicast group joining time. Instead of using multiple levels of flooding for group membership management, EGMP uses more efficient zonebased tree structure to allow nodes to quickly join and leave the group. EGMP introduces root zone and zone depth to facilitate simple and more reliable group membership management. EGMP does not use any periodic network-wide flooding, thus it can be scalable to both the group size and network size. Finally, a lot of work have been done on geocasting. Different from general multicasting, in which the destinations are a group of receivers, the destination of geocasting is one or multiple geographic regions (squares are normally defined). When packets reach the destined region, they will be sent to the nodes in the region through flooding or other methods. There is no need of forming multicast infrastructure to deliver packets to group members that may distribute widely in the whole network domain and change their positions as nodes move. We proposed an efficient and robust geographic multicast protocol for MANET. In this paper, we further introduce zone-supported geographic forwarding to reduce the routing failure, and provide mechanism to handle zone partitioning. In addition, we introduce a path optimization process to handle multiple paths, and provide a detailed cost analysis to demonstrate the scalability of the proposed routing scheme.

### III. Proposed Work

In this subsection, we present the multicast tree creation and maintenance schemes. In EGMP, instead of connecting each group member directly to the tree, the tree is formed in the granularity of zone with the guidance of location information, which significantly reduces the tree management overhead. With a destination location, a control message can be transmitted immediately without incurring a high overhead and delay to find the path first, which enables quick group joining and leaving. In the following description, except when explicitly indicated, we use  $G$ ,  $S$  and  $M$  respectively to represent a multicast group, a source of  $G$  and a member of  $G$ . When a multicast session  $G$  is initiated, the first source node  $S$  (or a separate group initiator) announces the existence of  $G$  by flooding a message  $NEW\ SESSION(G; zoneID)$  into the whole network. The message carries  $G$  and the ID of the zone where  $S$  is located, which is used as the initial root zone ID of group  $G$ . When a node  $M$  receives this message and is interested in  $G$ , it will join  $G$  using the process described in the next subsection. A

multicast group member will keep a membership table with an entry ( $G$ ; root  $zID$ ; isAked), where  $G$  is a group of which the node is a member, root  $zID$  is the root-zone ID and isAked is a flag indicating whether the node is on the corresponding multicast tree. A zone leader ( $zLdr$ ) maintains a multicast table. When a  $zLdr$  receives the  $NEW\ SESSION$  message, it will record the group ID and the root-zone ID in its multicast table. An example of one entry in the multicast table of node 16 is in fig. 3. The table contains the group ID, root-zone ID, upstream zone ID, downstream zone list and downstream node list. To end a session  $G$ ,  $S$  floods a message  $END\ SESSION(G)$ . When receiving this message, the nodes will remove all the information about  $G$  from their membership tables and multicast tables. When a node  $M$  wants to join the multicast group  $G$ , if it is not a leader node, it sends a  $JOIN\ REQ(M; PosM; G; fMoldg)$  message to its  $zLdr$ , carrying its address, position, and group to join. The address of the old group leader  $Mold$  is an option used when there is a leader handoff and a new leader sends an updated  $JOIN\ REQ$  message to its upstream zone. If  $M$  did not receive the  $NEW\ SESSION$  message or it just joined the network, it can search for the available groups by querying its neighbors. If a  $zLdr$  receives a  $JOIN\ REQ$  message or wants to join  $G$  itself, it begins the leader joining procedure as shown in Fig. 3. If the  $JOIN\ REQ$  message is received from a member  $M$  of the same zone, the  $zLdr$  adds  $M$  to the downstream node list of its multicast table. If the message is from another zone, it will compare the depth of the requesting zone and that of its own zone. If its zone depth is smaller, i.e., its zone is closer to the root zone than the requesting zone, it will add the requesting zone to its downstream zone list; otherwise, it simply continues forwarding the  $JOIN\ REQ$  message towards the root zone. If new nodes or zones are added to the downstream list, the leader will check the root-zone ID and the upstream zone ID. If it does not know the root zone, it starts an expanded ring search. As the zone leaders in the network cache the root-zone ID, a result can be quickly obtained. With the knowledge of the root zone, if its upstream zone ID is unset, the leader will represent its zone to send a  $JOIN\ REQ$  message towards the root zone; otherwise, the leader will send back a  $JOIN\ REPLY$  message to the source of the  $JOIN\ REQ$  message (which may be multiple hops away and the geographic uncasing described). When a node  $M$  wants to join the multicast group  $G$ , if it is not a leader node, it sends a  $JOIN\ REQ(M; PosM; G; fMoldg)$  message to its  $zLdr$ , carrying its address, position, and group to join. The address of the old group leader  $Mold$  is an option used when there is a leader handoff and a new leader sends an updated  $JOIN\ REQ$  message to its upstream zone. If  $M$  did not receive the  $NEW\ SESSION$  message or it just joined the network, it can search for the available groups by querying its neighbors. If a  $zLdr$  receives a  $JOIN\ REQ$  message or wants to join  $G$  itself, it begins the leader joining procedure as shown in Fig. 3. If the  $JOIN\ REQ$  message is received from a member  $M$  of the same zone, the  $zLdr$  adds  $M$  to the downstream node list of its multicast table. If the message is from another zone, it will compare the depth of the requesting zone and that of its own zone. If its zone depth is smaller, i.e., its zone is closer to the root zone than the requesting zone, it will add the requesting zone to its downstream zone list; otherwise, it simply continues forwarding the  $JOIN\ REQ$  message towards the root zone.

**Procedure *LeaderJoin*(*me*, *pkt*)***me*: the leader itself*pkt*: the JOIN\_REQ message the leader received**BEGIN****if** (*pkt.srcZone* == *me.zoneID*) **then**

/\* the join request is from a node in the local zone \*/

/\* add the node into the downstream node list of the multicast table \*/

AddNodeToMcastTable(*pkt.groupID*, *pkt.nodeID*);**else**

/\* the join request is from another zone \*/

**if** (*depth<sub>me</sub>* < *depth<sub>pkt</sub>*) **then**

/\* add this zone to the downstream zone list of the multicast table \*/

AddZoneToMcastTable(*pkt.groupID*, *pkt.zoneID*);**else**ForwardPacket(*pkt*);**return**;**end if****end if****if** (!LookupMcastTableForRoot(*pkt.groupID*)) **then**

/\* there is no root-zone information \*/

SendRootZoneRequest(*pkt.groupID*);**else if** (!LookupMcastTableForUpstream(*pkt.groupID*)) **then**

/\* there is no upstream zone information \*/

SendJoinRequest(*pkt.groupID*);**else**

SendReply;

**end if****END**

If new nodes or zones are added to the downstream list, the leader will check the root-zone ID and the upstream zone ID. If it does not know the root zone, it starts an expanded ring search. As the zone leaders in the network cache the root-zone ID, a result can be quickly obtained. With the knowledge of the root zone, if its upstream zone ID is unset, the leader will represent its zone to send a JOIN REQ message towards the root zone; otherwise, the leader will send back a JOIN REPLY message to the source of the JOIN REQ message (which may be multiple hops away and the geographic unicasting described of the JOIN REQ message receives the JOIN REPLY, if it is a node, it sets the isAked flag in its membership table and the joining procedure is completed. If the leader of a requesting zone receives the JOIN REPLY message, it will set its upstream zone ID as the ID of the zone where the JOIN REPLY message is sent, and then send JOIN REPLY messages to unacknowledged downstream nodes and zones. An example is given in fig. 1, in which the root zone of G is (2, 2), and the double circled nodes are zone leaders. Suppose currently zone (0, 0) and (1, 1) are not on the multicast tree, and their leader nodes 15 and 16 already know the root zone ID from the NEW SESSION message. Now node 15 plans to join G with the leader joining procedure. As it finds its upstream zone ID is unset, node 15 sends a JOIN REQ message towards root zone (2, 2). The message reaches zone (1, 1) and is intercepted by leader node 16, which then starts its leader joining procedure. Node 16 compares the depths of zone (0, 0) and its own zone. Since  $\text{depth}(0,0) = 2$  and  $\text{depth}(1,1) = 1$ ,  $\text{depth}(0,0) > \text{depth}(1,1)$ , node 16 adds zone ID (0, 0) to its downstream zone list. As node 16 finds its upstream zone ID is unset, it sends a JOIN REQ message towards the root zone. This message is received by the leader of the root-zone, node 3, and triggers the joining procedure of node 3. Node 3 adds the zone ID (1, 1) to its downstream zone list after comparing the depth. As the root zone does not have an upstream zone, node 3 sends back a JOIN REPLY message to the zone (1, 1). On receiving this message, node 16 sets the upstream zone ID as (2, 2) and sends a JOIN REPLY message to its unacknowledged downstream zone (0, 0). Node 15 sets its upstream zone as (1, 1) on receiving the JOIN REPLY message and the joining process is completed, with two multicast branches built between zones (2, 2) and (1, 1), and

between zones (1, 1) and (0, 0) respectively. Through the joining process, the group membership management is implemented in a distributed manner. An upstream zone only needs to manage its downstream zones, and the group membership of a local zone is only managed by its leader. The zone depth is used to guide efficient tree construction and packet forwarding.

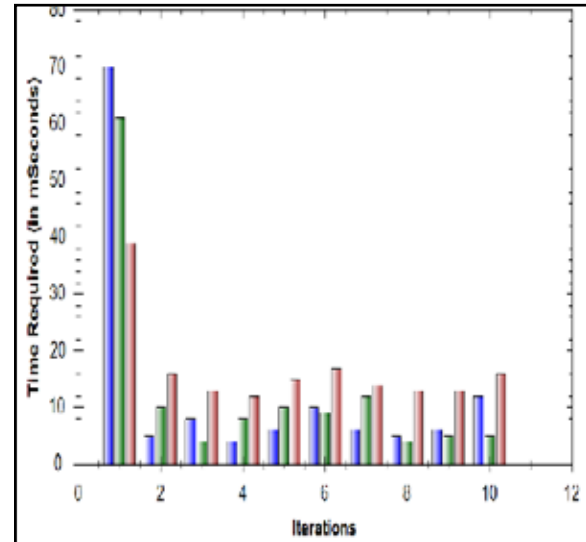
**IV. Results**

Fig. 1: Bar Chart on Basis on Time Complexity

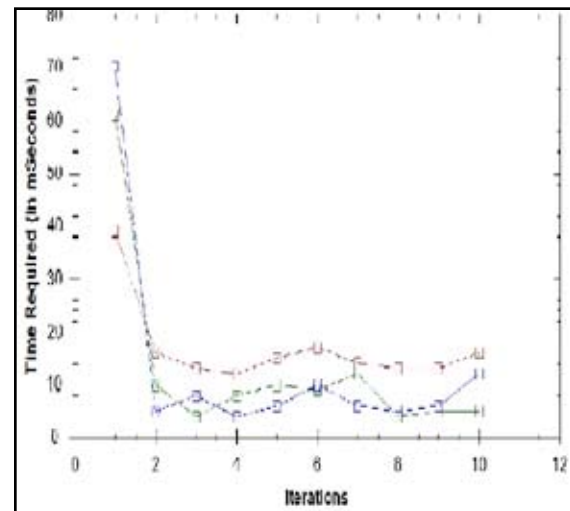


Fig. 2: Line Chart on Basis on Time Complexity

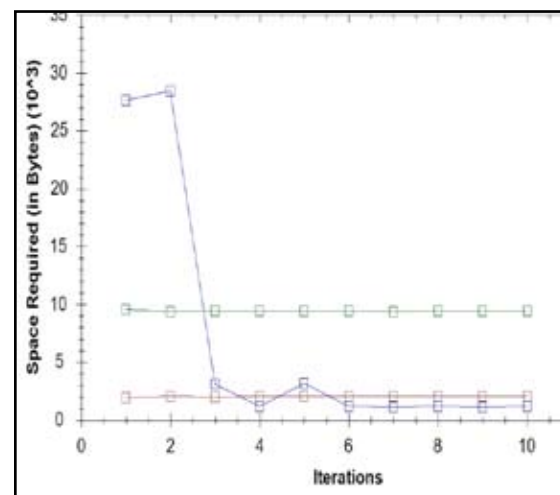


Fig. 3: Line Chart on Basis on Space Complexity

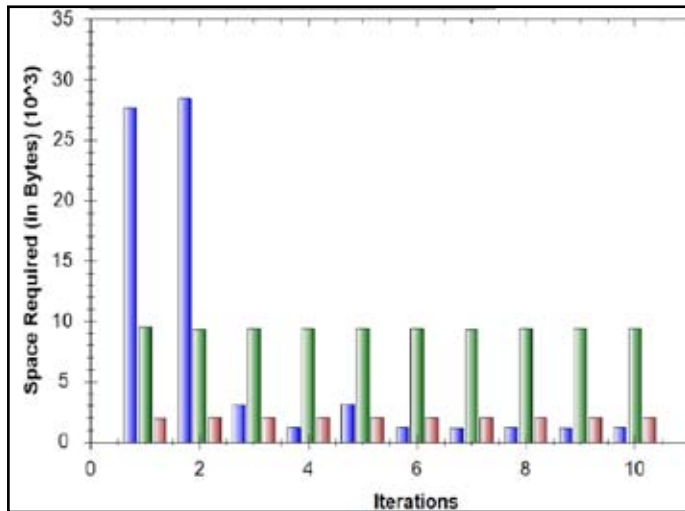


Fig. 3: Bar Chart on Basis on Space Complexity

## V. Conclusions

Group communications are important in Mobile Ad hoc Networks (MANET). Multicast is an efficient method for implementing group communications. However, it is challenging to implement efficient and scalable multicast in MANET due to the difficulty in group membership management and multicast packet forwarding over a dynamic topology. We propose a novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a virtual-zone-based structure to implement scalable and efficient group membership management. A network-wide zone-based bi-directional tree is constructed to achieve more efficient membership management and multicast delivery. The position information is used to guide the zone structure building, multicast tree construction and multicast packet forwarding, which efficiently reduces the overhead for route searching and tree structure maintenance. Several strategies have been proposed to further improve the efficiency of the protocol, for example, introducing the concept of zone depth for building an optimal tree structure and integrating the location search of group members with the hierarchical group membership management. Finally, we design a scheme to handle empty zone problem faced by most routing protocols using a zone structure. The scalability and the efficiency of EGMP are evaluated through simulations and quantitative analysis. Our simulation results demonstrate that EGMP has high packet delivery ratio, and low control overhead and multicast group joining delay under all test scenarios, and is scalable to both group size and network size. Compared to Scalable Position-Based Multicast (SPBM) [20], EGMP has significantly lower control overhead, data transmission overhead, and multicast group joining delay.

## References

- [1] S.S. Pradhan, J. Kusuma, K. Ramchandran, "Distributed Compression in a Dense Microsensor Network", IEEE Signal Processing Magazine, Vol. 19, No. 2, pp. 51-60, 2002.
- [2] A. Scaglione, S.D. Servetto, "On the Interdependence of Routing and Data Compression in Multi-Hop Sensor Networks", Proc. Eighth Ann. Int'l Conf. Mobile Computing and Networking, pp. 140-147, 2002.
- [3] N. Meratnia, R.A. de By, "A New Perspective on Trajectory Compression Techniques", Proc. ISPRS Commission II and IV, WG II/5, II/6, IV/1 and IV/2 Joint Workshop Spatial, Temporal and Multi- Dimensional Data Modelling and Analysis, 2003.

- [4] S. Baek, G. de Veciana, X. Su, "Minimizing Energy Consumption in Large-Scale Sensor Networks through Distributed Data Compression and Hierarchical Aggregation", IEEE J Selected Areas in Comm., Vol. 22, No. 6, pp. 1130-1140, 2004.
- [5] C.M. Sadler, M. Martonosi, "Data Compression Algorithms for Energy-Constrained Devices in Delay Tolerant Networks", Proc. ACM Conf. Embedded Networked Sensor Systems, 2006.
- [6] Y. Xu, W.C. Lee, "Compressing Moving Object Trajectory in Wireless Sensor Networks", Int'l J. Distributed Sensor Networks, Vol. 3, No. 2, pp. 151-174, 2007.
- [7] G. Shannon, B. Page, K. Duffy, R. Slotow, "African Elephant Home Range and Habitat Selection in Pongola Game Reserve, South Africa", African Zoology, Vol. 41, No. 1, pp. 37-44, 2006.
- [8] C. Roux, R.T.F. Bernard, "Home Range Size, Spatial Distribution and Habitat Use of Elephants in Two Enclosed Game Reserves in the Eastern Cape Province, South Africa", African J. Ecology, Vol. 47, No. 2, pp. 146-153, 2009.
- [9] J. Yang, M. Hu, "Trajpattern: Mining Sequential Patterns from Imprecise Trajectories of Mobile Objects", Proc. 10th Int'l Conf. Extending Database Technology, pp. 664-681, 2006.
- [10] M. Morzy, "Mining Frequent Trajectories of Moving Objects for Location Prediction", Proc. Fifth Int'l Conf. Machine Learning and Data Mining in Pattern Recognition, pp. 667-680, 2007.
- [11] F. Giannotti, M. Nanni, F. Pinelli, D. Pedreschi, "Trajectory Pattern Mining", Proc. ACM SIGKDD, pp. 330-339, 2007.
- [12] V.S. Tseng, K.W. Lin, "Energy Efficient Strategies for Object Tracking in Sensor Networks: A Data Mining Approach", J. Systems and Software, Vol. 80, No. 10, pp. 1678-1698, 2007.
- [13] L. Chen, M. Tamer Özsu, V. Oria, "Robust and Fast Similarity Search for Moving Object Trajectories", Proc. ACM SIGMOD, pp. 491-502, 2005.
- [14] Y. Wang, E.P. Lim, S.Y. Hwang, "Efficient Mining of Group Patterns from User Movement Data", Data Knowledge Eng., Vol. 57, No. 3, pp. 240-282, 2006.



Dr. K. Rama Krishnaiah is a highly qualified person holding M.Tech and Ph.D degree in CSE, an efficient and eminent academician. He is an outstanding administrator, a prolific researcher, who has published 21 research papers in various international journals and a forward looking educationist. He worked in prestigious K L University for 13 years and he contributed his service for NBA accreditation in May 2004, Aug 2007 with 'record rating', ISO 9001:2000 in 2004, Autonomous status in 2006, NAAC accreditation of UGC in 2008 and University status in 2009.



P. Prathiba has completed M.sc. from Andhara layola college vijayawada in 2005 and pursuing M.Tech in NOVA College of Engineering Technology for Women. Her research work includes concepts of Performance Evolution of Scalable, Multicasting over Mobile Ad-Hoc Networks.



Deevi. Harikrishna, received his M.Tech in Computer Science and Engineering from Acharya Nagarjuna University, and he completed M.Sc (CS) from Acharya Nagarjuna University.