Secured Multicasting Over MANET's through EGMP

1. **Mr.C.Narasimha,** (M.Tech)
c.narasimha522@gmail.com
2. **Mrs.B.Jalaja Kumari,** M.Tech
Asst.Professor dept of IT
Madanapalle Institute of Technology & Sciences, Madanapalle, Andhra Pradesh, India.

***Abstract*—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 Secured 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. To handle empty zone problem faced by most routing protocols using a zone structure. Finally, we design a scheme to handle security problem faced by multicasting. The scalability and the efficiency of EGMP are evaluated through simulations and quantitative analysis. Our 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) [15], EGMP has significantly lower control overhead, data transmission overhead, and multicast group joining delay.**

Index Terms— Routing, *wireless networks, mobile adhoc networks, multicasting, security, protocol*

1. Introduction

There are increasing interests and importance in supporting group communications over Mobile Ad Hoc Networks (MANETs). Example applications include the exchange of messages among a group of soldiers in a battlefield, communications among the firemen in a disaster area, and the support of multimedia games and teleconferences. With a one-to-many or many-to-many transmission pattern, multicast is an efficient method to realize group communications. However, there is a big challenge in enabling efficient multicasting over a MANET whose topology may change constantly.

Conventional MANET multicast protocols [2]–[7], [16] can be ascribed into two main categories, tree-based and meshbased. However, in MANET's nodes are not in a fixed position; nodes are always moving from one network to another network, it is very difficult to maintain the tree structure using these conventional tree-based protocols (e.g., MAODV [2], AMRIS [3], MZRP [4], and MZR [16]). The mesh-based protocols (e.g.FGMP [5], Core-Assisted Mesh protocol [6], ODMRP [7]) are proposed to enhance the robustness with the use of redundant paths between the source and the destination pairs. Conventional multicast protocols generally do not have good scalability due to the overhead incurred for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET.

For MANET unicast routing, geographic routing protocols [8]–[10] have been proposed in recent years for more scalable and robust packet transmissions. The existing geographic routing protocols generally assume mobile nodes are aware of their own positions through certain positioning system (e.g., GPS), and a source can obtain the destination position through some type of location service [11] [12]. In [9], an intermediate node makes its forwarding decisions 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 beaconing of the neighbors. By default, the packets are greedily forwarded to the neighbor that allows for the greatest geographic progress to the destination. When no such a neighbor exists, perimeter forwarding is used to recover from the local void, where a packet traverses the face of the planarized local topology subgraph by applying the right-hand rule until the greedy forwarding can be resumed. For example, in unicast geographic routing, the destination position is carried in the packet header to guide the packet forwarding, while in multicast routing, the destination is a group of members.

Besides requiring efficient packet forwarding, a scalable geographic multicast protocol also needs to efficiently manage the membership of a possibly large group, obtain the positions of the members and build routing paths to reach the members distributed in a possibly large network terrain. The existing small-group-based geographic multicast protocols [13]–[14] normally address only part of these problems.

In this work, we propose an efficient geographic multicast protocol, EGMP, which can scale to a large group size and large network size. The protocol is designed to be comprehensive and self-contained, yet simple and efficient for more reliable operation. Instead of addressing only a specific part of the problem, it includes a zone-based scheme to efficiently handle the group membership management, 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. By making use of the location information, EGMP could quickly and efficiently build packet distribution paths, and reliably maintain the forwarding paths in the presence of network dynamics due to unstable wireless channels or frequent node movements. In summary, our contributions in this work include:

1) Making use of the position information to design a scalable virtual-zone-based scheme for efficient membership management, which allows a node to join and leave a group quickly. Geographic unicast is enhanced to handle the routing failure due to the use of estimated destination position with reference to a zone and applied for sending control and data packets between two entities so that transmissions are more robust in the dynamic environment.

2) Supporting efficient location search of the multicast group members, by combining the location service with the membership management to avoid the need and over head of using a separate location server.

3) Introducing an important concept *zone depth*, which is efficient in guiding the tree branch building and tree structure maintenance, especially in the presence of node mobility. With nodes self-organizing into zones, zonebased bi-directional-tree-based distribution paths can be built quickly for efficient multicast packet forwarding.

4) Addressing the empty zone problem, which is critical in a zone-based protocol, through the adaption of tree structure.

5) The node want to send the packet then the node must do the encryption and then send the data to the zone leader.

6) Evaluating the performance of the protocol through quantitative analysis and extensive simulations. Our analysis results indicate that the cost of the protocol defined as the per-node control overhead remains constant regardless of the network size and the group size. Our simulation studies confirm the scalability and efficiency of the proposed protocol.

We organize the rest of this paper in the following sections .

2. Related Work

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.

In conventional topology multicast protocols mainly include tree based protocols (e.g., [2]–[4], [16]) and mesh-based protocols (e.g., [5], [7]). Tree structure is mainly constructed in tree based protocols for more efficient forwarding of packets to all the group members. With the help of mesh based protocols we can expand the multicast tree with additional paths which can be used to forward packets when some of the links break.

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. 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.

3. SECURED EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL

In this section we describe about implementation of secured EGMP protocol

3.1 Protocol Overview

EGMP supports scalable and reliable membership management and multicast forwarding through a two-tier *virtualzone- based* structure. At the lower tier the nodes are divided into zone. As shown in Fig. 1, and a leader is elected in a zone to manage the local group membership. At the upper layer, the leader serves as a representative for its zone to join or leave a multicast group as required. As result zone based, network-wide multicast tree is created. The zone leader can be elected based on the center point in the zone. The node which is present very close to the center of the zone that node can be act as a zone leader. Here the zone leader also have the mobility nature, if suppose the zone leader can change its position then again the zone leader election can be done based on the center point of the zone..

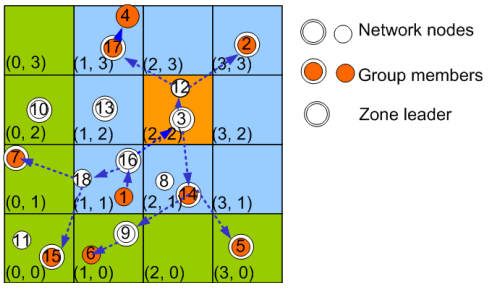

Fig 1: Zone structure and multicast session example

Some of the notations can be used:

Zone: The network terrain is divided into square zones as shown in Fig. 1.

S: Zone size, the length of a side of the zone square. The zone size is set to S≤ St/√2, where *St* is the transmission range of the mobile nodes. To reduce intra-zone management overhead, the intra-zone nodes can communicate directly with each other without the need of any intermediate relays.

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)/*s]*, b = [(*y-y0)/ s]*, where (*x*0*; y*0) is the position of the virtual origin, which can be a known reference location or determined at network setup time. A zone is *virtual* and formulated in reference to the virtual origin. For simplicity, we

assume all the zone IDs are positive *zone center*: For a zone with ID (a,b), the position of its center (*xc; yc*) can be calculated as:
xc = *x*0 + (*a*+ 0.5)* *r*, *yc* = *y*0 + (*b* + 0.5) * *r*. A packet destined to a zone will be forwarded towards 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 zones on the multicast tree. The tree zones are responsible for the multicast packet forwarding. A tree zone may have group members or just help forward the multicast packets for zones with members.
root zone: The zone where the root of the multicast tree is located.
zone depth: The depth of a zone is used to reflect its distance to the root zone. For a zone with ID (*a; b*), its depth is:
depth = max (| *a*0- *aj* | , | *jb*0 - *bj* |);
where (*a*0*; b*0) is the root-zone ID. For example, in Fig. 1, the root zone has *depth* zero, the eight zones immediately surrounding the root zone have *depth* one, and the outer seven zones have *depth* two.

3.2 Neighbor Table Generation and Zone Leader Election

For efficient management of states in a zone, a leader is elected with minimum overhead. As a node employs periodic BEACON broadcast to distribute its position in the underneath geographic unicast routing [9], to facilitate leader election and reduce overhead, EGMP simply inserts in the BEACON message a flag indicating whether the sender is a zone leader.
With zone size S=S≤St/√2, a broadcast message will be received by all the nodes in the zone. To reduce the beaconing overhead, instead of using fixed-interval beaconing, the beaconing interval for the underneath unicast protocol will be adaptive. A non-leader node will send a beacon every period of *Intvalmax* or when it moves to a new zone. A zone leader has to send out a beacon every period of *Intvalmin* to announce its leadership role.
A node constructs its neighbor table without extra signaling. When receiving a beacon from a neighbor, a node records the node ID, position and *flag* contained in the message in its neighbor table. Table 1 shows the neighbor table of node 18 in Fig. 1. The zone ID of the sending node can be calculated from its position, as discussed earlier. To avoid routing failure due to outdated topology information, an entry will be removed if not refreshed within a period *TimeoutNT* or the corresponding neighbor is detected unreachable by the MAC layer protocol.

nodeID	position	flag	zone ID
16	(x_{16}, y_{16})	1	(1, 1)
1	(x_1, y_1)	0	(1, 1)
7	(x_7, y_7)	1	(0, 1)
13	(x_{13}, y_{13})	1	(1, 2)

TABLE 1: The neighbor table of node 18 in Fig. 1

3.3 Multicast Tree Construction

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.

```
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 (depthme < depthpkt) 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
```

3.4 Multicast Packet Delivery

Here we discuss about packet forwarding to the nodes

3.4.1 Packet sending from the source

After the multicast tree is constructed, all the sources of the group could send packets to the tree and the packets will be forwarded along the tree. In most tree-based multicast protocols, a data source needs to send the packets initially to the root of the tree.

The source node want send the data to the members at that time we perform the security action, i.e. whenever the source node want to send the data , the source node can encrypt the data by using AES (Advanced Encryption Standers) the encrypted data can be transferred to the group members , in the transmission of packets the intermediate

nodes want to read the data , if suppose the nodes can access the data that time we don't have any problem because the data is in the encryption form i.e. cipher text , due to this text the intermediate nodes can't get the data it can simply transfer the data to the destination, in the destination side the receiver can decrypt the data using AES algorithm.
For providing the security we use the Advanced Encrypted Standards Algorithm

The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The strength of a 128-bit AES key is roughly equivalent to 2600-bits RSA key. AES data encryption is a more mathematically efficient and elegant cryptographic algorithm the time required to crack an encryption algorithm is directly related to the length of the key used to secure the communication (It takes less time). AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES (RSA). The algorithm was required to be royalty-free for use worldwide .AES has defined three versions, with 10, 12, and 14 rounds. Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits.

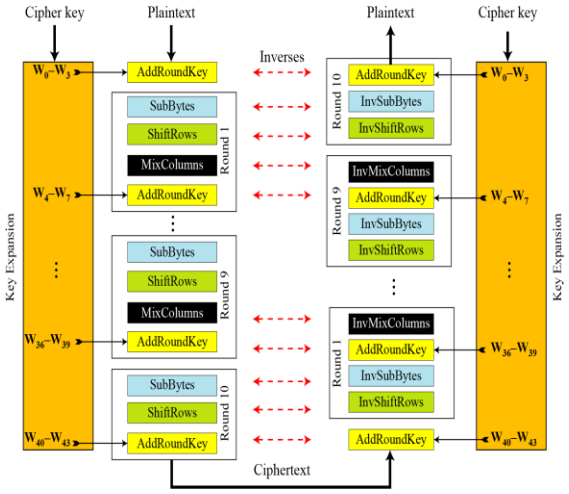

Fig2: **Ciphers and inverse ciphers of the original design**

AES was designed after DES. Most of the known attacks on DES were already tested on AES. AES is definitely more secure than DES due to the larger-size key. Numerous tests have failed to do statistical analysis of the cipher text. There are no differential and linear attacks on AES as yet. Numerous tests have failed to do statistical analysis of the cipher text.

In this section, some examples of encryption/ decryption and key generation are given The following shows the cipher text block created from a plaintext block using a randomly selected cipher key.

Plaintext:	00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19
Cipher Key:	24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87
Ciphertext:	BC 02 8B D3 E0 E3 B1 95 55 0D 6D FB E6 F1 82 41

Round	Input State	Output State	Round Key
Pre-round	00 12 0C 08	24 26 3D 1B	24 34 31 13
	04 04 00 23	71 71 E2 89	75 75 E2 AA
	12 12 13 19	B0 44 01 4D	A2 56 12 54
	14 00 11 19	A7 88 11 9E	B3 88 00 87
1	24 26 3D 1B	6C 44 13 BD	89 BD 8C 9F
	71 71 E2 89	B1 9E 46 35	55 20 C2 68
	B0 44 01 4D	C5 B5 F3 02	B5 E3 F1 A5
	A7 88 11 9E	5D 87 FC 8C	CE 46 46 C1
2	6C 44 13 BD	1A 90 15 B2	CE 73 FF 60
	B1 9E 46 35	66 09 1D FC	53 73 B1 D9
	C5 B5 F3 02	20 55 5A B2	CD 2E DF 7A
	5D 87 FC 8C	2B CB 8C 3C	15 53 15 D4
3	1A 90 15 B2	F6 7D A2 B0	FF 8C 73 13
	66 09 1D FC	1B 61 B4 B8	89 FA 4B 92
	20 55 5A B2	67 09 C9 45	85 AB 74 0E
	2B CB 8C 3C	4A 5C 51 09	C5 96 83 57
4	F6 7D A2 B0	CA E5 48 BB	B8 34 47 54
	1B 61 B4 B8	D8 42 AF 71	22 D8 93 01
	67 09 C9 45	D1 BA 98 2D	DE 75 01 0F
	4A 5C 51 09	4E 60 9E DF	B8 2E AD FA
5	CA E5 48 BB	90 35 13 60	D4 E0 A7 F3
	D8 42 AF 71	2C FB 82 3A	54 8C 1F 1E
	D1 BA 98 2D	9E FC 61 ED	F3 86 87 88
	4E 60 9E DF	49 39 CB 47	98 B6 1B E1
6	90 35 13 60	18 0A B9 B5	86 66 C1 32
	2C FB 82 3A	64 68 6A FB	90 1C 03 1D
	9E FC 61 ED	5A EF D7 79	0B 8D 0A 82
	49 39 CB 47	8E B2 10 4D	95 23 38 D9

4. Cost for the Protocol:

We summarize the per node cost of the protocol and validate our quantitative analysis through simulations

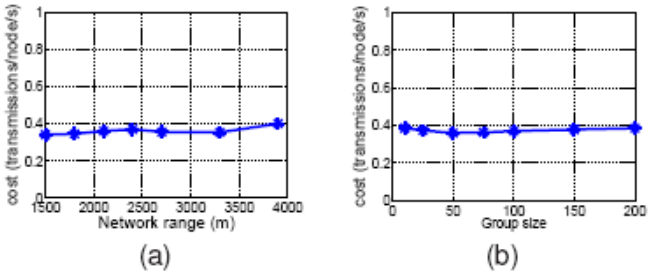

Fig 3: (a) Protocol cost vs. network size ; (b) Protocol cost vs. group size

4.1 Quantitative analysis on the per node cost

Theorem 1: The EGMP control overhead as the average number of control message transmissions per node every second has a complexity of O(1) with respect to the network

size and the group size.

Proof: The overhead of the protocol is generated from the tree construction and maintenance and the periodic beaconing in the underlying geographic unicast routing protocol. By Lemma 1, Lemma 3 and Eq. 2, the cost of the protocol, i.e., the number of transmissions of control messages per node every second with respect to the network size and the group size is:

$$\mathbf{Cost}_{\text{protocol}} = \mathbf{Cost}_{\text{tree}} + \mathbf{Cost}_{\text{maintain}} + \mathbf{Cost}_{\text{unicast}} = O(1)$$

4.2 Validation of the cost analysis by simulation

We validate our quantitative analysis on the protocol cost through simulations. The simulation settings and protocol Parameters were set as those in Section 5. We studied the protocol cost, i.e., the average number of transmissions of control messages by each node per second, with network size varied from 1500m *1500m with 156 nodes to 3900m * 3900m with 1056 nodes and the group size varied from 10 members to 200 members. Fig. 3(a) and (b) validate our quantitative analysis on the protocol cost. The protocol cost keeps almost constant between 0.3 and 0.4 with different network sizes and group sizes. The above analysis results indicate that when the network size and the group size increase, the control overhead placed on each node per second by the protocol will remain relatively constant. Next, we will further demonstrate the scalability and efficiency of the protocol by simulation studies.

4.3 Cost for maintaining the Security

The algorithms used in AES are so simple that they can be easily implemented using cheap processors and a minimum amount of memory.

5. CONCLUSION

There is an increasing demand and a big challenge to design more secure, scalable and reliable multicast protocol over a dynamic ad hoc network (MANET). In this paper, we propose a secured efficient and scalable geographic multicast protocol, EGMP for MANET. The scalability of EGMP is achieved through a two-tier virtual-zone-based structure. A zone-based bi-directional multicast tree is built at the upper tier . 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 this protocol is very secured by using AES with that we transmit the data in dynamic mobile adhoc networks very securely, by using these secured EGMP we can transmit the data efficiently and securely to the destination.

Our results indicate that geometric information can be used to more efficiently construct and maintain multicast structure, and to achieve more secure, scalable and reliable multicast transmissions in the presence of constant topology change of MANET. Our simulation results demonstrate that secured 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 Scalable Position-Based Multicast (SPBM) [15], EGMP has significantly lower control overhead, data transmission overhead, and multicast group joining delay.

6.References

[1] X. Xiang, X. Wang, and Y. Yang. Supporting efficient and scalable multicasting over mobile adhoc networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 4, April 2011

[2] E. M. Royer and C. E. Perkins. Multicast operation of the ad hoc on-demand distance vector routing protocol. in *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, August 1999, pp. 207218.

[3] C. Wu, Y. Tay, and C.-K. Toh. Ad hoc multicast routing protocol utilizing increasing id-numbers (AMRIS) functional specification. *Internet draft*, November 1998.

[4] X. Zhang and L. Jacob. Multicast zone routing protocol in mobile ad hoc wireless networks. in *Proceedings of Local Computer Networks*, 2003 (LCN 03), October 2003.

[5] C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol (FGMP) for multihop mobile wireless networks In *AJ. Cluster Comp, Special Issue on Mobile Computing*, vol. 1, no. 2, pp. 187196, 1998.

[6] J. J. Garcia-Luna-Aceves and E. Madruga. The core-assisted mesh protocol. In *IEEE JSAC*, pp. 13801394, August 1999.

[7] M. Gerla, S. J. Lee, and W. Su. On-demand multicast routing protocol (ODMRP) for ad hoc networks. in *Internet draft*, draft-ietf-manet-odmrp- 02.txt, 2000.

[8] X. Xiang, Z. Zhou and X. Wang. Self-Adaptive On Demand Geographic Routing Protocols for Mobile Ad Hoc Networks. *IEEE INFOCOM07 minisymposium*, Anchorage, Alaska, May 2007.

[9] B. Karp and H. T. Kung. Greedy perimeter stateless routing for wireless networks. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, pages 243–254, August 2000.

[10] F. Kuhn, R. Wattenhofer, Y. Zhang and A. Zollinger. Geometric ad-hoc routing: Of theory and practice. In *Int. Symposium on the Principles of Distributed Computing (PODC)*, 2003.

[11] J. Li and et al. A scalable location service for geographic ad hoc routing. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, pages 120–130, 2000.

[12] S. Giordano and M. Hamdi. Mobility management: The virtual home region. In *Tech. report*, October 1999.
[13] S. Basagni, I. Chlamtac, and V. R. Syrotiuk, Location aware, dependable multicast for mobile ad hoc networks, Computer Networks, vol. 36, no. 5-6, pp. 659670, August 2001.
[14] M. Mauve, H. Fubler, J. Widmer, and T. Lang. Position-based multicast routing for mobile ad-hoc networks. In *Poster section in ACM MOBIHOC*, June 2003
[15] M. Transier, H. Fubler, J. Widmer, M. Mauve, and W. Effelsberg. A Hierarchical Approach to Position-Based Multicast for Mobile Ad-hoc Networks. In Wireless Networks, vol. 13 no. 4, Springer, pp. 447-460, August 2007
[16] V. Devarapalli and D. Sidhu. MZR: A multicast protocol for mobile ad hoc networks. In *ICC 2001 Proceedings*, 2001.
[17] E.Madhusudhana Reddy, M.Padmavathamm Need for Strong Public KeyCryptography in Electronic Commerce in International journal of Computer Applications in Engineering Technology and Sciences. IJ-CA-ETS (ISSN: 0974-3596), PP 58-68, 2009.
[18] E.Madhusudhana Reddy, M. Padmavathamma An Information Security Model for E-Business in The Technology World Quarterly Journal , Volume V, Issue I, PP 203-206, 2009.