Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient and Secured Multicasting Over MANET's Through EGMP

[1]Mr.C.Narasimha (M.Tech),
[2]Mrs.M. Sreedevi M.Tech, (Ph.D)
Computer Science & Engineering
[2]Assoc. Professor, Dept of *C. S.E*
[1,2]Madanapalle Institute of Technology & Science,
Madanapalle, Andhra Pradesh, India
c.narasimha522@gmail.com

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. We design a scheme to handle security problem faced by multicasting. Finally, we design to maintain the data in the buffer of the zone leader to send the data to the crashed node. 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.

In this work, we propose an efficient geographic multicast protocol, EGMP, which can scale to a large group size and large network size. 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.

© 2012, IJARCSSE All Rights Reserved

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]) 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 *virtual zone- 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.

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 $S \leq St/\sqrt{2}$, 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.

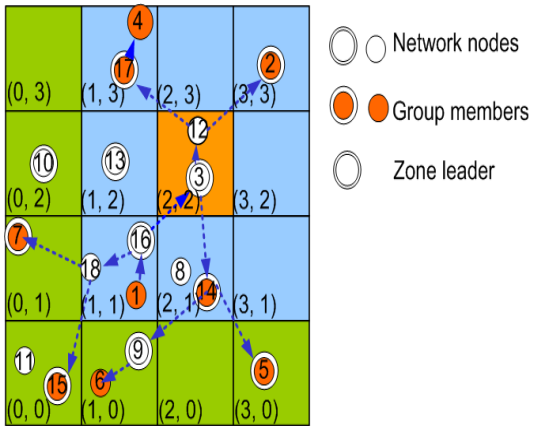

Fig 1: Zone structure and multicast session example

Zone ID: The identification of a zone. A node can calculate its zone ID (a, b) from its position coordinates (x, y) as:

$a = [(x\text{-}x0)/s]$, $b = [(y\text{-}y0)/s]$, where $(x0; y0)$ 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:

$xc = x0 + (a + 0.5) * r$, $yc = y0 + (b + 0.5) * r$. 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:

$depth = \max(|a0 - aj|, |jb0 - bj|)$;

where $(a0; b0)$ 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 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

© 2012, IJARCSSE All Rights Reserved

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;
        endif
    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
```

3.3 Multicast Packet Delivery

Here we discuss about packet forwarding to the nodes

3.3.1 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.

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.

```
Procedure data delivery(gId,nId)
/*   gId : the group id is represent group name and node
position
/*   nId : node of a particular group  */
BEGIN
        /* a node want to do multicasting then it require
the node information      */
        If(!zoneledcreated)then
            /* if node information not present then it sen a
request to the zone leader    */
            sendJoin(gId);
        else if(!node information)then /* if zone leader is
not created  */
              sendRequest(gId);
             else /* the node has the information it can
take data and call aes() function*/
              aes();
              return();
            end if
       end if
END
```

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

3.4 Crash node send recovery message:-

In MANET's mobile nodes are dynamically change its location, the main drawback of the mobile node is, it can have a less capacity to hold the power. That means the mobile nodes or wireless nodes are run with the help

© 2012, IJARCSSE All Rights Reserved

of the power, if the power get lost the mobile nodes are not live, these nodes are temporarily crashed or not worked. Not only had the loss of power in any conditions if the node gets crashed the data loosed. The node can't leave the zone i.e. it cannot change its location it can't noted to the zone leader to its absence, so unfortunately the zone leader can maintain the node information to its database, so due to this what happen means the nodes which want to send the data to another node it can take the information from the zone leader and select the nodes to send the data , in that selected nodes one of the selected nodes is the crashed node so at that time the data can reached to all the destination nodes except the crashed node, the data get lost, the zone leader can recognized that which node is not received the data , now zone leader can decided that , the node get crashed, so for overcoming the loss of data , the zone leader can maintain one temporary buffer to store the data.

Now the zone leader can store the data, whenever the crash node can recovered that node can send the message to the zone leader the message consists of node get live, and then the zone leader can send the data to that recovery node.

4. 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.

The efficient data delivery of the zone leader can increase the performance of the nodes due to less involvement in the communication, i.e. once source node can send the data its job is over, remaining all things can be taken by the zone leader to handle efficient data deliver, so due to this data cannot get lost.

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. 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] 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

[12] C.Narasimha , B.Jalaja Kumari , Secured Multicasting Over MANTE's through EGMP, AITM, vol.1, no.2, pp.90-96, 2012

© 2012, IJARCSSE All Rights Reserved