ASYMMETRICALLY SECURED EGMP OVER MANET'S

Sayed Mohammed Raja, Seetha. R, Arun Kumar S
School of Information Technology,
VIT University, Vellore,India
Email: sayedmohammedraja@gmail.com, aarunkumar889@gmail.com

Abstract— Group communications are significant in Mobile Ad hoc Networks (MANET). Multicast is an well-organized technique for applying group communications. Yet, it is interesting to implement effective and accessible multicast in MANET due to the effort in group member management and multicasting of packets forwarding in an active topology. We suggest a Asymmetrically Secured novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a practical-zone-based arrangement to implement accessible and effective group member management. A network-wide zone-based bi-directional tree is made to attain more well-organized member management and multicast delivery. The location information is used to monitor the zone structure, multicast tree building and multicast packets forwarding, which capably reduce the overhead for route finding and tree structure maintenance. Some approaches have been suggested to further improvement in the efficiency of the protocol, for example, presenting the concept of zone depth for construction an ideal tree structure and adding the position search of group of members with the ordered group member management. To switch empty zone problem met by most routing protocols using a zone structure. Finally, we plan a pattern to switch the security problem faced by the multicasting. The scalability and the productivity of EGMP are assessed through simulations and quantitative analysis. Our results prove that EGMP has great packet delivery ratio, and low control overhead, and is accessible to both group size and network size. EGMP has expressively lower control overhead, data transmission overhead, and multicast group joining delay.

1. Introduction

The growing benefits and significance in associating group communication on Mobile Ad Hoc Networks (MANETs). For example presentations include the conversation of messages between a set of warriors in a theatre of war, communications between the firemen in a danger, and the support of multimedia games and teleconferences. By a one-to-many or many-to-many communication pattern, multicast is an capable method to understand group communications. Though, there is a great challenge in allowing efficient multicasting over a MANET whose topology changes continuously.

Conventional MANET multicast protocols can be endorsed into two main categories,

Tree-based and mesh-based. Conversely, in MANET's nodes are not in a stable location; nodes are continuously move from one network to another, it is very tough to keep the tree structure by these conservative tree-based protocols (e.g., MAODV, AMRIS, MZRP). The mesh based protocols (e.g. FGMP, ODMRP) are suggested to improve the strength with the usage of terminated routes among the source and the destination pairs. For MANET uni-cast routing, geographical routing protocols have been suggested for more accessible and robust packet broadcasts. The current geographical routing protocols assume that the mobile nodes know their own locations through certain locating system (e.g., GPS), and a source can find the destination location through certain type of location service .An transitional node marks its forwarding conclusions based on the destination position introduced in the packet header by the source and the locations of its one-hop neighbour's. By default, the packets are insatiably promoted to the neighbour which allows for the extreme geographical growth to the destination. Once no such neighbour occurs, forwarding used to improve from the local void, where a packet crosses the face of the local topology sub-graph by using the right-hand rule up to the greedy forwarding can be continued. For example, in uni-cast routing, the destination location is carried in the packet header to guide the packet forwarding, whereas in multicast routing, the destination is a group of members. Moreover demanding well-organized packet forwarding, a scalable geographic multicast protocol also desires to manage the membership of a large group, attain the locations of the members and construct routing paths to reach to the members circulated in a probably large network environment. The present small-group-based geographic multicast protocols usually report only share these difficulties. In this work, we suggest an efficient geographic multicast protocol, EGMP, which can balance to a large group size and large network size. The protocol is considered to be wide-ranging and independent, yet simple and well-organized for more consistent operation. Instead of mentioning only a exact part of the problem, it also includes a zone-based system to capably switch the group membership management,

In summary, our contributions in this work include:

1) Making use of the location info to project a accessible effective-zone-based system for well-organized membership management, which permits a node to join and leave a group rapidly. Geographic uni-cast is improved to switch the routing failure due to the usage of predictable destination location with orientation to a zone and practical for transfer control and data packets among two nodes thus communications are more robust in the active environment.

2) By supporting the well-organized location exploration of the multicast group members, by joining the position service with the membership management to escape the requirement and overhead by means of a distinct location server.

3) By Presenting a significant theory *zone depth*, which is well-organized in controlling the tree outlet building and tree structure conservation, particularly in the occurrence of node mobility? With nodes self-establishing into zones, zone-based bi-directional-tree-based supply routes can be made rapidly for well-organized multicast packet forwarding.

4) By addressing the empty zone problem, this is serious in a zone-based protocol, through the conversion of tree structure.

5) If the node needs to send the packet then the node should do the encryption and then send the data to the zone leader.

6) Estimating the presentation of the protocol through quantitative analysis and extensive simulations. Our analyses consequences indicate that the cost of the protocol

2. Related Work

In this part, we review the fundamental measures believed in conservative multicast protocols, and subsequently commence a little geographic multicast algorithms projected in the literature. In conservative topology multicast protocols mostly embrace tree based protocols and mesh based protocols example Tree structure is generally constructed in tree based protocols for supplementary well-organized forwarding of packets to all the group members. By the help of mesh based protocols we can develop the multicast tree with extra paths that can be used to forward packets when some of the links break.

3. SECURED EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL

In this part we explain about implementation of secured EGMP protocol

3.1 Protocol synopsis

EGMP supports scalable and consistent membership management and multicast forwarding during a two-tier *effective zone- base* structure. At the lower tier the nodes are separated into zones. As shown in Fig. 1 and a leader is chosen in a zone to control the local group membership. At the upper layer, the leader serves as a agent for its zone to join or leave a multicast group as necessary. As consequence zone based, network-wide multicast tree is produced. The zone leader can be chosen based on the centre point in the zone. The node which is their very close up to the centre of the zone that node can be performed as a zone leader. Here the zone leader also has the mobility nature, Assume the zone leader be able to modify its location then again the zone leader choice can be prepared based on the centre point of the zone.

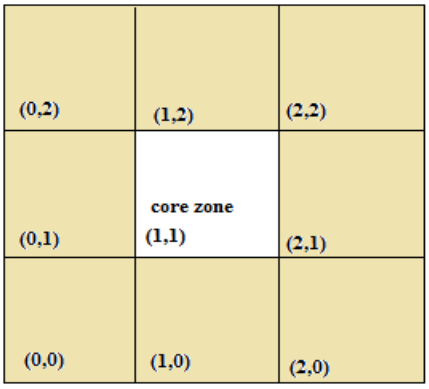


Fig 1: Zone structure and multicast session example

Some of the notations can be used:

Zone: The network property is separated into square zones as shown in Fig. 1.

S: Zone size, the measurement length wise of a side of the zone square. The zone size is set to S≤St/√2, where *St* is the communication scope of the mobile nodes. To decrease intra-zone management overhead, the intra-zone nodes are able to communicate openly with each other not including the need of any transitional relays.

Zone ID: The identification of a zone. A node be able to determine 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 location of the virtual origin, which can be a well-known reference position. A zone is *essential* and formulate in orientation to the practical origin. For ease, we suppose all the zone IDs are positive *zone centre*: For a zone with ID (a, b), the location of its centre (*xc; yc*) can be calculated as: *xc* = *x*0 + (*a*+ 0.5)* *r*, *yc*= *y*0 + (*b* + 0.5) * *r*. A packet meant to a zone will be forwarded just before the centre of the zone.

ZLdr: Zone leader. A zLdr is selected in all zones for supervision 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 dependable 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 Neighbour Table creation and Zone Leader Election

For well-organized management of states in a zone, a leader is elected with smallest amount of transparency. As a node employ interrupted BEACON transmit to issue its location in the beneath geographic uni-cast routing, to ease leader election and condense transparency, EGMP just insert in the BEACON message a flag signifying whether the sender is a zone leader.

With zone size S=S≤St/√2, a transmit message will be received by all the nodes which are in the zone. To decrease the beaconing transparency, instead of using rigid-interval beaconing, the beaconing interval for the beneath uni-cast protocol will be adaptive. A non-leader node will send a beacon every time of *Intvalmax*or when it moves to a new zone. A zone leader has to send out a beacon every time of *Intvalmin* to declare its leadership responsibility.

A node can construct its neighbour table not including the extra signalling. While reception of a beacon from a neighbour, a node files the node ID, location and *flag* contain in the message in its neighbour table. Table 1 shows the neighbour table of node 18 in Fig. 1. The zone ID of the sending node can be designed from its location, as discussed earlier. To stay away from routing failure due to redundant topology information, an access will be isolated if not revived surrounded by a period *TimeoutNT* or the subsequent neighbour is detected inaccessible by the MAC layer protocol

Node ID	Position	Flag	Zone ID
9	(x_9,y_9)	1	(0,0)
8	(x_8,y_8)	0	(1,0)
2	(x_2,y_2)	1	(2,2)
7	(x_7,y_7)	1	(0,1)

Table 1 The neighbour table represents for node 18

3.3 Multicast Tree creation

The multicast tree creation and maintenance schemes are mentioned. In EGMP, instead of linking 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.

3.4 Multicast Packet Delivery

3.4.1 Packet sending

If a source wants to deliver a packet on the multicast tree, first the source should join in to the multicast tree and should become a member in the group. Like other multicast geographic protocols EGMP doesn't use single-direction tree, it uses Bi-directional tree i.e. the packets flow will be not only in one direction from

Upstream nodes to downstream nodes and also from downstream nodes to upstream nodes. But in many protocols which are based on core zone should send the packets to core zone, but in some cases it leads to more delay for example from figure the node 5 is far away to the core zone if node 5 should send the packet to core zone due to the far distance it incur more delay, because if the distance of source is to large from the core zone then delay will be increased, so to reduce delay the packet is sent on to the tree directly. once the multicast tree is created, all the sources of the group could send packets to the tree and the packets will be forwarded all along the tree. In generally tree-based multicast protocols, a data source wants to transmit the packets primarily to the root of the tree. The source node desire to send the data to the members at that time we do the security action, i.e. when the source node want to transmit the data , the source node can encrypt the data by using RSA (Rivest, Adi Shamir and Len Adleman) the data can be transfer to the group members , in the broadcast of packets the transitional nodes want to read the data ,The data is in the encryption form i.e. cipher text , the text the middle nodes can't get the data it can just transmit the data to the destination, in the destination side the receiver can decrypt the data using RSA algorithm. To provide the security we use the RSA Algorithm which can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Key Generation Algorithm

1. Generate two big casual primes, p and q, of about identical range such that their product n = pq is of the essential bit length, e.g. 1024 bits.

2. Calculate n = pq and phi = (p-1)(q-1).

3. Prefer an integer e, 1 < e < phi, such that gcd (e, phi) = 1.

4. Calculate the undisclosed exponent d, 1 < d < phi, such that ed = 1 (mod phi).

5. The public key is (n, e) and the private key is (n, d). Maintain all the values d, p, q and phi undisclosed.

Parameter Description:

- n is recognized as the modulus.
- e is recognized as the public exponent or encryption exponent or just the example.
- d is recognized as the undisclosed exponent or decryption exponent.

Encryption Algorithm

Sender A does the subsequent:-

- Obtain the recipient B's public key (n, e).
- Represent the simple text message as a positive integer m.
- Calculates the cipher text c = me mod n.
- Transmit the cipher text c to B.

Decryption Algorithm

Recipient B accomplishes the subsequent:-

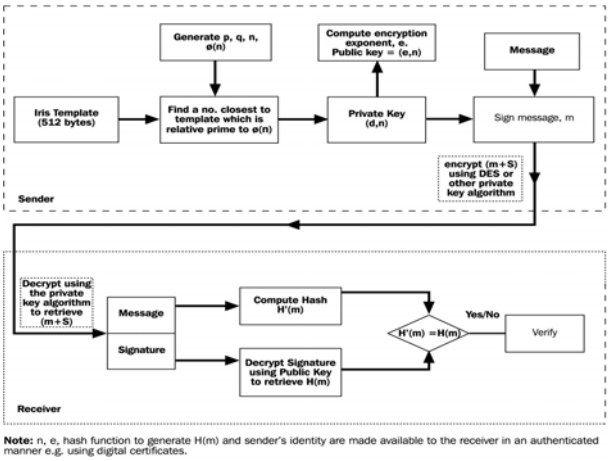
- Use its private key (n, d) to calculate m = cd mod n.
- Remove the simple text from the message m.

Signature verification

Recipient B accomplishes the subsequent:-

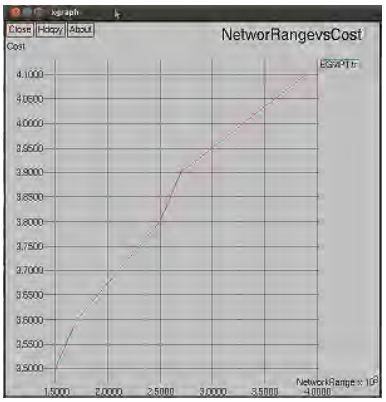
- Use correspondent A's public key (n, e) to calculate integer v = se mod n.
- Remove the message commencing this integer.
- Autonomously calculates the message of the information that has been signed.

Suppose both the messages are alike, the signature is legitimate.



4. Cost for the Protocol

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



(a)

(b)

Fig2. Presentation of EGMP with dissimilar group size (a) Network range vs. cost (b) Group vs. cost

4.1 Quantitative analysis on the per node cost

The EGMP manage transparency as the standard number of control message transmission per node every second has a complexity of O (1) with respect to the network size and the group size. The overhead of the protocol is generated from the tree construction and maintenance and the periodic beaconing in the underlying geographic uni-cast routing protocol. The number of transmissions of control messages per node every second with respect to the network size and the group size is:

Protocol cost = Tree construction cost +Tree maintenance cost + Cost of uni -cast = O (1)

4.2 Cost for maintaining the Security

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

5. CONCLUSION

On the way to generate further security, scalable and consistent multicast protocol in a active ad hoc network (MANET). In this paper, we recommend a secured well-organized and scalable geographical multicast protocol, EGMP for MANET. The scalability of EGMP is achieved during a two-tier virtual-zone-based structure. A zone-based bi-directional multicast tree is built at the higher tier. The location information is used in the protocol to direct the zone arrangement and construction, multicast tree structure, safeguarding, and multicast packet forwarding. compare to the conservative topology based on multicast protocols, the use of the position information in EGMP extensively reduce the tree structure and preservation transparency, and enable faster tree construction to the network topology alteration. Moreover to extend a format to switch the empty zone problem, this is demanding for the zone-based protocols. Moreover, EGMP makes use of geographic forwarding for reliable packet transmission, and capably track the location of multicast group members exclusive of resorting to an exterior position server. We formulate this protocol is very protected by using RSA with that we broadcast the information in self-motivated ad-hoc networks very strongly, by means of the available EGMP we can broadcast the information capably and securely to the target.

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 adhoc wireless networks. In *Proceedings of Local Computer Networks*, 2003(LCN 03), October 2003.C. Narasimha &B. Jalaja Kumari, AITM, Vol. 1, No. 2, pp. 90-96, 2012 96

[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, and 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 mini symposium*, 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 adhoc 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