Secure Efficient GEOGRAPHIC Multicast Protocol For Mobile AdHoc Networks

Jyoti M.Karbhal , Kishor B. Sadafale
Student, ME (Information Technology)
Sinhgad College of Engineering, Pune, India,
Assistant Professor (Information Technology)
Sinhgad College of Engineering ,Pune, India,

Abstract— A mobile ad-hoc network (MANET) is composed of mobile nodes without any infrastructure. So that Ad hoc networks are mainly used in emergency situations where no infrastructure is available, for e.g. military battlefields, disaster mitigation, emergency search, rescue sites, classrooms and conventions, where participants share information dynamically using their mobile devices. These applications lend themselves well to multicast operations. In addition, within a wireless medium, it is even more crucial to reduce the transmission overhead and power consumption. Multicasting can improve the efficiency of the wireless link when sending multiple copies of messages by exploiting the inherent broadcast property of wireless transmission. Scalability is important issue in term of group size and network size while designing multicast protocol. In addition security is an essential requirement in MANET environments. Compared to Wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eavesdropping, limited power and bandwidth, and dynamic network topology. Efficient Geographic Multicasting Protocol (EGMP) came into existence to implement group communication in MANET. Efficient Geographic Multicast Protocol (EGMP) uses a virtual-zone-based structure to implement scalable and efficient group membership scheme. The efficiency and scalability of the protocol was already tested but security aspect is not considered. To further improve the efficiency of the protocol, we propose a Secure Efficient Geographic Multicast Protocol (SEGMP).In this paper we study comparative analysis of simple mesh topology using ADOV, EGMP and SEGMP and test average delay, throughput, packet delivery ratio, energy.

Keywords- *Mobile ad-hoc network (MANET) , group ,Multicast routing protocol, Scalability,Security,RSA.*

I. INTRODUCTION

Multicast is the delivery of a message or information to a group of destinations simultaneously in a single transmission using routers, only when the topology of the network requires it. Multicasting is an efficient method in realize group communications with a one-to-many or many-to-many relationship transmission pattern. However, there is a big challenge in enabling efficient multicasting over a MANET whose topology may change constantly. Conventional MANET multicast protocol divided into two main category i) Topology based multicast protocol (stateful) ii) Position based multicast protocol (stateless) .

Topology-based multicast protocols for mobile ad-hoc networks can be categorized into two main classes: tree-based and mesh-based protocols. The tree-based approaches build a data dissemination tree that contains exactly one path from a source to each destination. Topological information is used for its construction. The trees can be sub-classified further into source trees and shared trees. E.g. MZR[1]. In these protocols, each single source builds its own tree to distribute its packets. In contrast to that, a shared tree is one in which each connected node is able to send packets to all other nodes using the same tree. Shared trees are built among others E.g. MAODV [2]. Tree-based approaches often use local repair mechanisms to shield the distribution structure from link failures caused by mobility. Mesh-based approaches, building meshes of data paths to make the multicast routes more stable against topological changes. This comes at the expense of a higher overhead during data delivery. A mesh can contain multiple possible paths from a source to a destination. E.g. ODMRP [3], FGMP [4].Drawback of 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.

Second category is position based multicast protocol. In location-based multicast routing protocols, Each node determines its own location through the use of the availability of a Global Positioning System (GPS), Bluetooth or other locations systems easily s when required [5]. A location service is used by the sender of a packet to determine the location of the destination. The routing decision at each forwarding node is then based on the location information of its neighbors and the destination nodes. E.g. DSM [6], LGT [7]. Drawback of geographic multicast protocols like DSM [6], LGT [7] is these protocol used only for small groups. As these protocol 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, these protocols are not scalable. So we have to focus on scalability aspect as well as security which is not focused in above protocol. MANET is vulnerable to many attacks like wormhole attack, blackhole attack, Denial of Service attack, flooding attack [8, 9] .

In this work, we propose a Secure Efficient Geographic Multicast Protocol, SEGMP, which work against flooding or Denial of Service attack and improve the performance of existing protocol.

II. RELATED WORK

Most of the research work is focus on unicasting compared to multicasting in MANET hence multicasting in mobile ad hoc networks is a relatively unexplored research area. Also research work related to security attacks in MANET focus on unicasting only. So more research required on the effects of security attacks on multicasting in MANET and scalability of multicast protocols. Here we focus on some protocol which focus on scalability aspect.

Like stateless or position based protocol Hierarchical Rendezvous Point multicast (HRPM) [10] also used location information that is available from the Global Positioning System (GPS) or localization algorithms. But, existing location based multicast protocols are not scalable to large groups. As group size increased, the per-packet encoding overhead, and the centralized group membership and location management become more difficult for large group size. HRPM is designed to overcome these issues. HRPM uses two key concept two support large group sizes 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. HRPM recursively partitions a large multicast group into manageable sized subgroups so that tree-encoding overhead limits to the application-specified constant (ω). HRPM introduce two logical entities AP (Access Point) and RP (rendezvous point). Where all members in cell is managed by cell's AP (Access Point) and entire region has an RP. Thus HRPM maintain two level hierarchy. But some of the drawbacks of this protocol are 1) In HRPM nodes need to hash RP, and for calculating RP it assumes that every node knows network size which is very difficult for dynamic network . 2) There is some additional challenges due to mobility of the nodes. It causes frequent RP handoff. 3) Increase mobility also increases the chance of RP search inconsistency and failure. 4) When any node want to join group it first send join request to RP, which will increase joining delay.

Another protocol which focus scalability issue is Scalable Position-Based Multicast (SPBM) [11] protocol uses the geographic position of nodes to support large group size. SPBM forward the data packet with a very low overhead . SPBM is robust to changes in the topology of the network. To achieve this SPBM uses the concept of quad tree where entire network is subdivided into a quad-tree with a predefined maximum level of aggregation L. Single squares are identified by their concatenated level-n to level-1 square number. 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. So when the network size increases due to membership flooding significant control overhead will be generated. In addition in SPBM any membership change of a node may need to go through L levels to make it known to the whole network. This leads to a long multicast group joining time. Instead of using multiple levels of flooding for group membership management, SEGMP uses more efficient zone based tree structure as in existing EGMP protocol to allow nodes to quickly join and leave the group . And also perform secure data transmission by avoiding flooding or Denial of Service attack using RSA technique.

III. SECURE EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL(SEGMP)

A. Protocol Overview

SEGMP supports scalable and reliable membership management and multicast forwarding through a two-tier virtual zone based structure. At the lower layer, in reference to a predetermined virtual origin, the nodes in the network self organize themselves into a set of zones, 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 [12]. As a result, a network-wide zone-based multicast tree is built. For efficient and reliable management and transmissions, location information will be integrated with the design and used to guide the zone construction, group membership management, multicast tree construction and maintenance, and packet forwarding. The zone-based tree is shared for all the multicast sources of a group. Some of the notations to be used are:

Zone: The network terrain is divided into square zones.

Zone size is r, such that $r <= rt/\sqrt{2}$ where rt is transmission range. So that all nodes in zone are in communication range with each other.

Zone ID: The identification of a zone. zone ID (a, b) Calculated as $a=x-x_0/2$ $b=y-y_0/2$ where (x, y) is position coordinates of node and (x_0,y_0) predefine reference origin.

Zone centre: zone center (xc, yc) can be calculated as $x_c= x_0 + (a+ 0.5)*r$, $y_c= y_0 + (a+ 0.5)*r$.

Root zone: The zone where the root of the multicast tree is located.

B. Zone leader election

In each zone node nearer to zone center having maximum energy become a zone leader. To elect the zone leader each node broadcast its position, energy, flag indicating whether it is zone leader every period of maxInterval. All nodes maintain zone table which consist node id, energy and flag of other zone member. Each node check zone table period of minInterval and hence node nearer to zone center having maximum energy declare itself as zone leader by setting flag equal to 1. Zone leader announce its leadership every period of minInterval.

C. Multicast Tree construction and data forwarding

When a multicast session G is initiated by source node S. It broadcast NEW_SESSION message containing group id and its location into the whole network. A zone where source node is situated is called as root zone. After receiving NEW_SESSION message, Node M wants to join the multicast group G sends a JOIN_REQ message to its zone leader first. Root zone leader send JOIN_REPLY message to the member and complete the joining process. Hence multicast tree is constructed in granularity of zones. 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. Instead, EGMP assumes a bidirectional-tree based forwarding strategy, with which the multicast packets can flow not only from an upstream node/zone down to its downstream nodes /zones but also from a downstream node/zone up to its upstream node/zone.

D. Authentication Scheme

The MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority. Denial of Service is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. So before sending packets authentication must be done, so the improper nodes or intruders are avoided from the network. Here we RSA technique for authentication. The security of the RSA cryptosystem depends on the difficulty of factoring large integers. Three main steps of the RSA Algorithm are: 1) Key generation: The prime numbers (p) and (q) are chosen and multiplied together to form (n), an encryption exponent (e) is chosen, and the decryption exponent (d) is calculated using the following rules: Compute z by the equation, z = (p-1) (q-1). 2) Select a small odd integer d that is relatively prime to z. 3) Compute e by the equation, e × d = 1 mod z. 4) Publish the pair (e, n) as the RSA public key and keep secret the pair (d, n) as private key. 5) Encryption: The message (M) is raised to the power (e), and then reduced modulo (n). So, the encrypted message $C = M^e \bmod n$.6) Decryption: The cipher text (C) is raised to the power (d), and then reduced modulo (n) and the decrypted message (original message) is found by $M = C^d \bmod n$.

In our SEGMP before sending the data node has to authenticate itself first. To do that every node share some secrete key. When sender node want to send data it first encrypt secrete key with public key of receiver node and send it to receiver. Receiver decrypt it with private key and check secrete key if it is same receiver allow sender to send data otherwise it detect as intruder and avoided from network.

IV. RESULT AND DISCUSSION

We implement four modules in ns2 as listed below to evaluate performance of SEGMP

MODULE1: Implementation of mesh topology using AODV protocol.

In this module we implement mesh topology using exisisting AODV protocol. Data's are transmitted between the source and destination. The protocol evaluation is based on a simulation of 50 wireless nodes forming an ad hoc network, moving about over a rectangular (500 m x 500 m) flat space. The nodes in the simulation move according to a random waypoint model. In the simulation, Constant Bit-Rate (CBR) traffic flows are used. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs.

MODULE 2: Implementation of a Wireless Tree topology using the newly implemented EGMP protocol

In this module we implement wireless tree topology using the newly implemented EGMP protocol as discussed earlier and data's are transmitted between the source and destination. The protocol evaluation is based on a simulation of 50 wireless nodes forming an ad hoc network, moving about over a rectangular (500 m x 500 m) flat space. The nodes in the simulation move according to a random waypoint model. In the simulation, Constant Bit-Rate (CBR) traffic flows are used. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs.

MODULE 3: Implementation of a Wireless Tree topology using the newly implemented EGMP protocol with attacker node.

In this module we implement wireless tree topology using the newly implemented EGMP protocol with attacker node. Here we insert one node which performs DoS attack by flooding. The protocol evaluation is based on a simulation of 51 wireless nodes forming an ad hoc network, moving about over a rectangular (500 m x 500 m) flat space. The nodes in the simulation move according to a random waypoint model. In the simulation, Constant Bit-Rate (CBR) traffic flows are used. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs.

MODULE4: Implementation of a Wireless Tree topology using secure EGMP protocol.

In this module we implement wireless tree topology using secure EGMP protocol. Each node before sending the packet must authenticate itself using RSA technique as discussed earlier, so the improper node or intruder is avoided from network. Here we insert one node which performs DoS attack by flooding. The protocol evaluation is based on a simulation of 51 wireless nodes forming an ad hoc network, moving about over a rectangular (500 m x 500 m) flat space. The nodes in the simulation move according to a random waypoint model. In the simulation, Constant Bit-Rate (CBR) traffic flows are used. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs. The corresponding Packet Delivery Ratio, Energy consumption and the Delay is calculated and the output is plotted in graphs.

MODULE5: Comparison of above four modules.

Comparison of the above four modules are done on energy, delay, throughput and the Packet Delivery Ratio and the output's are plotted using graphs.

Average delay:

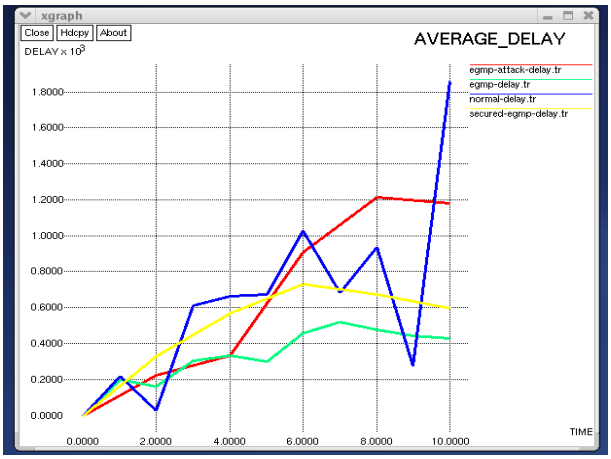

Figure 1. Average delay

Figure 1 shows average delay over time. With mesh topology using AODV (blue color) its varying over time. With tree topology using EGMP (green color) it is minimum. In EGMP with attacker (red color) delay is increased as compared to EGMP and in secure EGMP (yellow color) it is minimum with compared to EGMP with attacker but as compared to plain EGMP it is slightly increased due to encryption decryption computation.

Throughput:

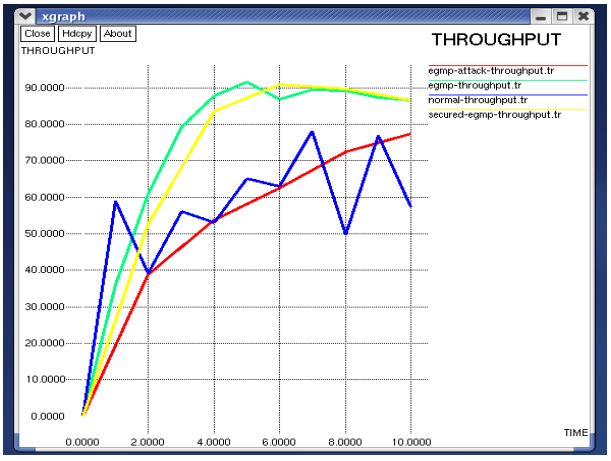

Figure 2 Throughput

Figure 2 shows throughput over time. With mesh topology using AODV (blue color) it is minimum compared to tree topology using EGMP (green color). In EGMP with attacker (red color) throughput is decreased as compared to EGMP and in secure EGMP (yellow color) we get almost same throughput as in plain EGMP. Hence using secure EGMP we maintain the performance of EGMP.

Packet Delivery Ratio:

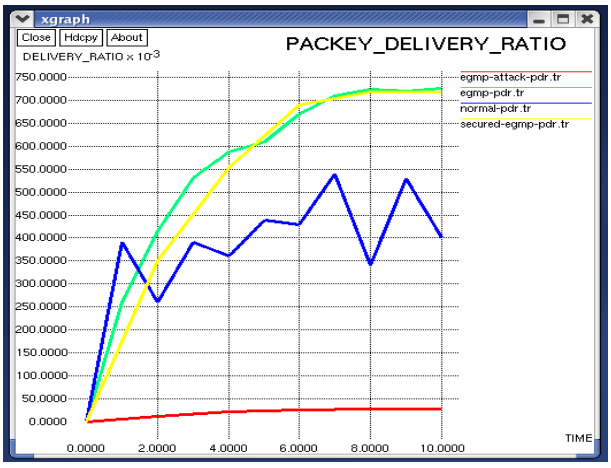

Figure 3. Packet Delivery Ratio

Figure 3 shows packet delivery ratio over time. With mesh topology using AODV (blue color) it is minimum compared to tree topology using EGMP (green color). In EGMP with attacker (red color) packet delivery ratio is much decreased as compared to EGMP and in secure EGMP (yellow color) we get almost same packet delivery ratio as in plain EGMP.Hence using secure EGMP we maintain the performance of EGMP.

Energy:

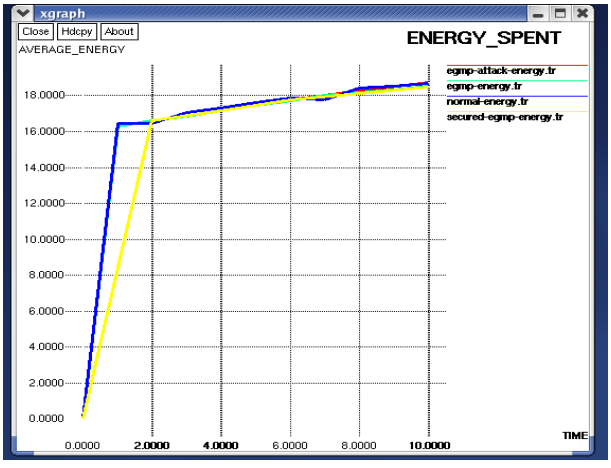

Figure 4. Energy spent

Figure 4. shows energy spent over time. As shown in graph energy spent in each module is almost same there is no much difference in energy spent.

V. CONCLUSION

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 a Secure efficient and scalable geographic multicast protocol, SEGMP, for MANET. Compare to other protocol like SPBM and HRPM ,SEGMP is more scalable and Secure. It Support efficient multicast membership management and data delivery. It reduces the tree construction and maintenance overhead, as compared to conventional topology-based multicast protocols.

REFERENCES

[1] V. Devarapalli and D. Sidhu, "MZR: A Multicast Protocol for Mobile Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '01), 2001.

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

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

[4]C.-C. Chiang, M. Gerla, and L. Zhang, "Forwarding Group Multicast Protocol (FGMP) for Multichip Mobile Wireless Networks,"ACM J. Cluster Computing, special issue on mobile computing, vol. 1, no. 2, pp. 187-196, 1998.

[5] E. Kaplan, Understanding GPS. Artech House, 1996.

[6]S. Basagni, I. Chlamtac, and V.R. Syrotiuk, "Location Aware, Dependable Multicast for Mobile Ad Hoc Network", Computer Networks,vol.36,nos5-6,pp. 659-670,Aug. 2001.

[7] K. Chen and K. Nahrstedt, "Effective Location-Guided Tree Construction Algorithms for Small Group Multicast in MANET,"Proc.IEEE INFOCOM, pp. 1180-1189, 2002.

[8] Arunmozhi Annamalai, Venkataramani Yegnanarayanan,"Secured System against DDoS Attack in Mobile Adhoc Network" WSEAS TRANSACTIONS on COMMUNICATIONS, ISSN: 2224-2864 Issue 9, Volume 11, September 2012

[9] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay," Different Types of Attacks on Integrated MANET-Internet Communication" International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265

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

[11]M. Transier, H. Fubler, J. Widmer, M. Mauve, and W. Effelsberg,"A Hierarchical Approach to Position-Based Multicast for Mobile Ad-Hoc Networks," Wireless Networks, vol. 13, no. 4, pp. 447-460,Aug. 2007.

[12] X. Xiang, Member, IEEE, X. Wang, Member, IEEE, and Y. Yang," Efficient and Scalable Multicasting over mobile Ad Hoc Networks", IEEE Trans. MOBILE COMPUT.ING, VOL. 10, NO. 5, APRIL 2011