G. Ramya Reddy, C.Swapna, R. Durga Gopal, P.Veeranath / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.1669-1674

Security Enhancement Using Rsa Algorithm In Multicast Manet

G. Ramya Reddy[1], C.Swapna[2], R. Durga Gopal[3], P.Veeranath[4]
[1] *Graduate from Joginpally B.R. Engg College,HYd, India*
[2]*Assistant Professor of ECE Dept, Joginpally B.R.Engg College,Hyd, India*
[3,4] *Associate Professor of ECE Dept, Joginpally B.R.Engg College,Hyd, India*

Abstract

In mobile ad hoc networks, an application scenario requires mostly collaborative mobility behaviour. The key problem of those applications is scalability with regard to the number of multicast members as well as the number of the multicast group. To enhance scalability with group mobility, we have proposed a multicast protocol based on a new framework for hierarchical multicasting that is suitable for the group mobility model in MANET. We propose a advanced privacy policy by using a secret key Transformation by using RSA algorithm in novel Secured Geographic Multicast Protocol (SGMP). SGMP internally uses the Efficient Geographic Multicast Protocol (SGMP) 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 SGMP are evaluated through simulations and quantitative analysis.

Keywords—RSA, wireless Sensor networks, mobile adhoc networks.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. *Ad hoc* is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networks have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

A. Architecture of ad hoc network

Basically ad hoc network is a On-demand Distance Vector (AODV) routing protocol which is reactive in nature at the same time it is stateless protocol to ascertain the routers as per the route request (RREQ) and rote reply (RREP) source node information. Initially internet is used as a main head of the architecture to control and transfer the data to the routers with complete QoS, multimedia, security of access networks.

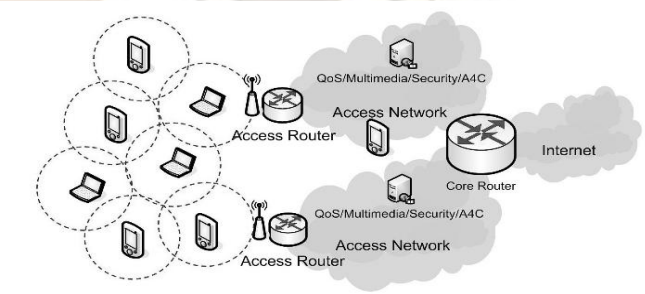


Fig. 1: shows the ad hoc network architecture

Thus transferred information to the access routers is further transferred to clients or customers as in the figure below. As per the construction features of an ad hoc network architecture all the primary users that is clients and agents receive the information through the base station (towers), this infrastructure is supported by certain spectrum bands present at the primary users. Further the network information can be formulated in the path of routing protocols with wireless sensor networks, mesh networks and mobile ad hoc networks so as to remove overlapping areas, without any of the central

controllers or reorganization of network infrastructure.

According to Eurescom (N.A) access provided for the future networks with limitless services provided to small coverage areas of WLAN hotspot and flexibility by ad hoc networks is reliable. Features of ad hoc networks are QoS, security, authentication, authorization and charging. Utilizing the features ad hoc network can perform several functionalities. From the figure it is observed that the internet connection through core routers is supplied with all features to the networking access routers. Each and every operator in the network may obtain a single IP address with perfect routing mechanisms for supporting the mobility users. The differentiation, admission control and recovery participation of mobility usage with all the terminals connected back of ad hoc networks as well as major challenges where supported by QoS. Servers present in the operator's management networks and security are modified by the ad hoc resources.

II. ENSURING LOCATION PRIVACY IN MOBILE AD HOC NETWORKS

One solution is the Flying Freedom System (Escudero-Pascual, Heidenfalk and Heselius, 2001), where a set of protected extensions in the mix-based Freedom System architecture were introduced to permit a mobile node to seamlessly roam among IP subnetworks and media types while remaining untraceable and pseudonymous. This solution is illustrated in fig 2 below. Now, when a user is roaming among different foreign networks, the home agent only knows that it is forwarding messages to the Flying Freedom server (FF in the figure). After passing an anonymous communication network based on Chaumian Mixes, the request is eventually forwarded to the foreign agent (denoted FA).

Fig. 2: Using the Flying Freedom System to achieve location privacy

III. RSA ALGORITHM

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

B. Operation

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[4]
5. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
   - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption)

exponent *d*, which must be kept secret. *p*, *q*, and φ(*n*) must also be kept secret because they can be used to calculate *d*.

Encryption

Alice transmits her public key (*n*, *e*) to Bob and keeps the private key secret. Bob then wishes to send message *M* to Alice.

He first turns *M* into an integer *m*, such that 0 ≤ *m* < *n* by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext *c* corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits *c* to Alice.

C. *Decryption*

Alice can recover *m* from *c* by using her private key exponent *d* via computing

$$m = c^d \pmod{n}.$$

Given *m*, she can recover the original message *M* by reversing the padding scheme.

IV. ZONE BASED STRUCTURE AND MULTICAST SESSION

In 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 zone based tree structure to allow nodes to quickly join and leave the group.

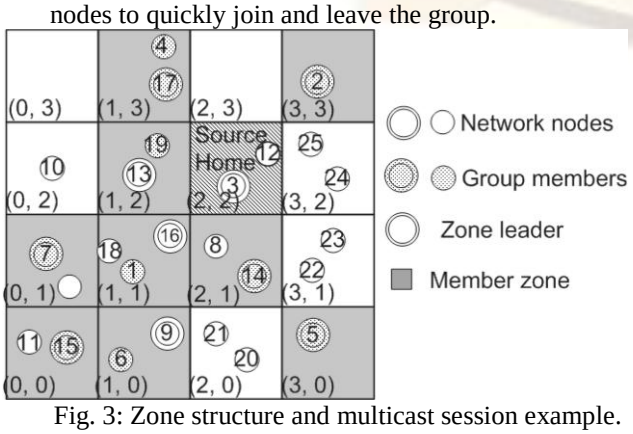


Fig. 3: Zone structure and multicast session example.

V. SECURED GEOGRAPHIC MULTICAST PROTOCOL

D. *Introduction to Secured Geographic Multicast Protocol*

In this section, we will describe the SGMP protocol in details. We first give an overview of the protocol and introduce the notations to be used in the rest of the paper, we present our designs for the construction of zone structure and the zone-based geographic forwarding. Finally, we introduce our mechanisms for multicast tree creation, maintenance and multicast packet delivery.

E. *Protocol Overview*

SGMP 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 pre-determined virtual origin, the nodes in the network self-organize themselves into a set of zones 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 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. To further reduce the forwarding overhead and delay, EGMP supports bi-directional packet forwarding along the tree structure. That is, instead of sending the packets to the root of the tree first, a source forwards the multicast packets directly along the tree. At the upper layer, the multicast packets will flow along the multicast tree both upstream to the root zone and downstream to the leaf zones of the tree. At the lower layer, when an on tree zone leader receives the packets, it will send them to the group members in its local zone.

Many issues need to be addressed to make the protocol fully functional and scalable. The issues related to zone management include: the schemes for more efficient and robust zone construction and maintenance, the strategies for election and maintenance of a zone leader with minimum overhead, zone partitioning as a result of severe wireless channels or signal blocking, potential packet loss when multicast members move across zones. The issues related to packet forwarding include: the efficient building of multicast paths with the zone structure, the handling of empty zone problem, the efficient tree structure maintenance during node movements, the reliable transmissions of control and multicast data packets, and obtaining location information to facilitate our geometric design without

resorting to an external location server. For the convenience of presentation, we first introduce the terminologies used in the paper. In EGMP, we assume every node is aware of its own position through some positioning system (e.g., GPS) or other localization schemes. The forwarding of data packets and most control messages is based on the geographic unicast routing protocol GPSR. SGMP, however, does not depend on a specific geographic unicast protocol.

F. 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.

G. Multicast session initiation and termination

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; zoneIDS*) into the whole network. The message carries G and the ID of the zone where S is located, which is used as the initial *rootzone* 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; isAcked*), where G is a group of which the node is a member, root zID is the root-zone ID and isAcked 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. Table 2 is an example of one entry in the multicast table of node 16 in Fig. 1. 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.

TABLE I
THE ENTRY OF GROUP *G* IN MULTICAST TABLE OF NODE 16

group ID	G
root-zone ID	$(2, 2)$
upstream zone ID	$(2, 2)$
downstream zone list	$(0, 1)$, $(0, 0)$
downstream node list	1

H. Pseudocode for The Leader Joining Procedure

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
```

I. Moving between different zones

When a member node moves to a new zone, it must rejoin the multicast tree through the new leader. When a leader is moving away from its current zone, it must handover its multicast table to the new leader in the zone, so that all the downstream zones and nodes will remain connected to the multicast tree. Whenever a node M moves into a new zone, it will rejoin a multicast group G by sending a JOIN REQ message to its new leader. During this joining process, to reduce the packet loss, whenever the node broadcasts a BEACON message to update its information to the nodes in the new zone, it also uncast a copy of the message to the leader of its previous zone to update its position.

Since it has not sent the LEAVE message to the old leader, the old leader will forward the multicast packets to M. This forwarding process helps reduce the packet loss and facilitates seamless packet transmissions during zone crossing. When the

rejoining process finishes, M will send a LEAVE message to its old leader.

To handle leader mobility problem, if a leader finds its distance to the zone border is less than a threshold or it is already in a new zone, it assumes it is moving away from the zone where it was the leader, and it starts the handover process. To look for the new leader, it compares the positions of the nodes in the zone it is leaving from and selects the one closest to the zone center as the new leader. It then sends its multicast table to the new leader, which will announce its leadership role immediately through a BEACON message. It will also send a JOIN REQ message to its upstream zone.

During the transition, the old leader may still receive multicast packets. It will forward all these packets to the new leader when the handover process is completed. If there is no other node in the zone and the zone will become empty, it will use the method introduced in the next subsection to deliver its multicast table. In the case that the leader dies suddenly before handing over its multicast table, the downstream zones and nodes will reconnect to the multicast tree through the maintenance process described.

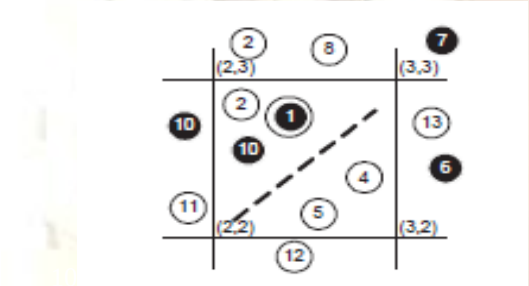


Fig. 3: Multiple clusters in one zone.

VI. SIMULATION AND RESULTS

The programming language used to design and implementation of code is MATLAB. The reason for using MATLAB in this project is due to its signal processing and communication toolbox that helped to obtain an efficient code.

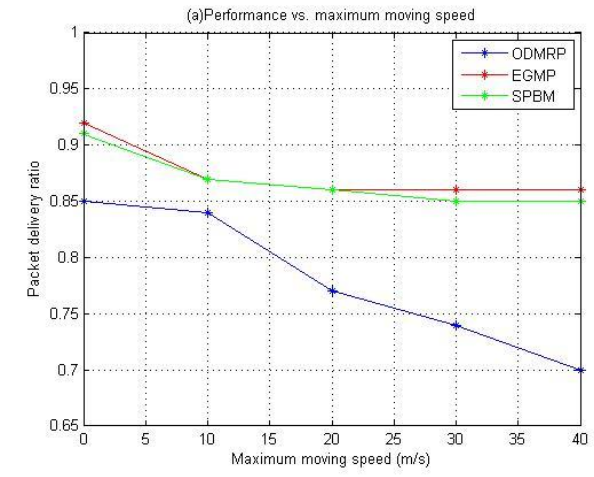
J. Performance Evaluation

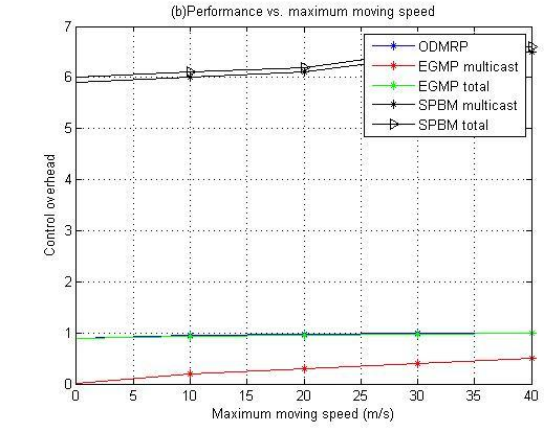
We implemented the SGMP protocol using Global Mobile Simulation (GloMoSim) library, and compare it with ODMRP which is widely used and considered to be robust over a dynamic network, and the geographic multicast protocol SPBM which is designed to improve the scalability of position-based multicast. The SPBM is a quad-tree-based protocol as introduced in ODMRP is a mesh based on-demand non-geographic multicast protocol, and takes a soft state approach to maintain multicast group members.

A multicast source broadcasts Join_Query messages to the entire network periodically. An intermediate node stores the source ID and the sequence number, and updates its routing table with the node ID (i.e. backward learning) from which the message was received for the reverse path back to the source. A receiver creates and broadcasts a Join Reply to its neighbors, with the next hop node ID field filled by extracting information from its routing table.

K. Normalized control overhead

The total number of control message transmissions divided by the total number of received data packets. Each forwarding of the control message was counted as one transmission. Different from ODMRP, EGMP and SPBM are based on Some underlying geographic unicast routing protocol which involves use of periodic beacons. To provide more insight on the performance of different protocols, we measured both the total overhead (including multicast overhead and unicast overhead) and multicast overhead for EGMP and SPBM (represented as EGMP-multicast and SPBM-multicast).





VII. CONCLUSIONS

New developments of anonymity technologies are needed to adapt existing solutions to the new challenging area of mobile *ad hoc* networks. For example, the scenarios assumed a sound anonymous overlay network in the mobile *ad hoc* domain that both provides strong anonymity and

fits the characteristics of mobile *ad hoc* networks. Compared to conventional topology based multicast protocols; the use of location information in SGMP significantly reduces the tree construction and maintenance overhead, and enables quicker tree structure adaptation to the network topology change. By Using RSA algorithm the security become increased when compared to normal Transmission. We also develop a scheme to handle the empty zone problem, which is challenging for the zone-based protocols. Additionally, SGMP 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 SGMP protocol and our results indicate that the per-node cost of SGMP keeps relatively constant with respect to the network size and the group size. We also performed extensive simulations to evaluate the performance of SGMP.

REFERENCES

[1] H. Kopka and P.W. Daly, *A Guide to LATEX*, third ed. Harlow, U.K.: Addison-Wesley, 1999.IEEE Transactions On Mobile Computing 16

[2] L. Ji and M. S. Corson. Differential destination multicast: a MANET multicast routing protocol for small groups. In *Proc. IEEE Infocom01*, Anchorage, Alaska, April 2001.

[3] 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.

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

[5] 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.

[6] http://en.wikipedia.org/wiki/RSA_(algorithm)

[7] http://en.wikipedia.org/wiki/Mobile Adhoc Network

G. Ramya Reddy, She Obtained her B.Tech from Joginpally B.R. Engineering College.

C.Swapna, She obtained her M.Tech from Hi-Tech College of Engineering College, Hyderabad. Currently working as a Assistant Professor in Joginpally B.R. Engineering College. She guided many B.Tech and M.Tech students to improve their Knowledge.

R.Durga Gopal, He obtained his M.Tech from CVR College of Engineering College, Hyderabad and pursuing Ph.D from JNTUH. Currently working as a Associate Professor in Joginpally B.R. Engineering College, His area of research includes Signal Processing, Communications and VLSI. In his career he guided so many B.Tech and M.Tech students to improve their Knowledge.

P.Veeranath, He obtained his M.Tech from SNIST, Hyderabad and pursuing Ph.D from JNTUH. Currently working as a Associate Professor in Joginpally B.R. Engineering College, His area of research includes Signal Processing, Communications and GPS. In his career he guided so many B.Tech and M.Tech students to improve their Knowledge.