ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Enhanced Group Key Management in Mobile Adhoc Networks

Shruthi Karuru

M.TECH in Computer Networks, Shree Devi Institute of Technology, Kenjar, Mangalore, Karnataka, India

Abstract: Mobile adhoc network (MANET) is an integration of nodes where a node can be sender, recipient or relay and may be unaware until they come in contact with each other. Communication in such a network should be secured as topology, bandwidth, network size, resources etc. changes. The core aspect of establishing secured communication can be done with the help of authentication check by exchanging keys. In this paper, we propose a novel approach for group key management scheme by simple rekeying technique on frequent scalable and high mobility nodes.

Keywords: Group key management (GKM); Mobile ad hoc network (MANET); rekeying approach;

I. INTRODUCTION

A MANET is a type of adhoc network that can change locations and configurations or any node can join or leave the network at any point of time. It is dynamic in nature which frequently changes its topology and communication among the nodes takes place using wireless connections.
Security of a network becomes an important factor when constructing the network. A network must achieve security requirements like authentication, confidentiality, integrity, and availability which rely on the availability of secure key management system in network.

Group key management (GKM) system involves creation and distribution of keys for all the group members. It issues keys to the nodes to encrypt/decrypt the messages, and to prevent the improper use of legally issued keys. Absence of key management system makes a network vulnerable to several attacks. Therefore, key management system is the basic and important need of a network for secure communication.

The features of MANETs such as dynamic topology, lack of centralized authority, resource constrained and node mobility are the major challenges in establishment of key management where a group of members can send and receive messages, in a way that outsiders are unable to access any information even when they are able to intercept the messages.

II. GROUP KEY MANAGEMENT PROTOCOLS IN MANETS

Here are the GKM protocols of mobile adhoc network:

- *Centralized protocol*: In this approach, a single entity is responsible for controlling the whole group and group rekeying.
- *Decentralized protocol*: In this approach, multiple entities are responsible for managing the group as opposed to a single entity.
- *Distributed protocol*: In this approach, group members themselves contribute to the formation of a group key and are equally responsible for the rekeying and distribution of group keys.

III. EXISTING METHODS

Three GKM protocols are considered namely, centralized group key distribution (CGKD), decentralized group key management (DGKM) and distributed group key distribution (DGKD).

In CGKD, it uses a group controller (GC) as a central entity for generating, distributing and updating the group key. It uses key tree scheme or logical key hierarchy (LKH) ,where root node specifies group participant or user in its tree structure that reduces number of broadcasting messages over the root and leaf nodes. The user shares a pair wise key with group initiator as well as a set of intermediate keys from leaf to the root.

The DGKM scheme involves dividing a large group into number of small subgroups. The subgroup controller in every subgroup manages the keys. Every group member contributes a share in forming a final common group key. The key is refreshed or updated in response to the changes of group membership.

The DGKD introduces the concept of sponsors and co distributors. It does not use any central entity but allows all the group members to have the capability and are equally trusted. It allows any group member to become sponsor of other members or co-distributor. Sponsor of member initiates and distributes the keys to the co-distributors once a key generated. The co-distributor in turn distributes to the corresponding members. The rekeying process is initiated by the sponsor whenever a member joins or leaves the network.

IV. PROPOSED METHOD

The proposed method is based on the distributed protocol. Here the nodes are positioned in four different quadrants

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

and can roam from one quadrant to another. Thus different group key is generated for each quadrant using Prime number and each node of respective quadrant is assigned a unique key using Euler's φ( ). The group key (GK) and keys (K) of each node is updated whenever a new node joins or leaves the network. Communication between the nodes can be done using multiplicative encryption algorithm.

The flow chart of this method is shown in figure1.

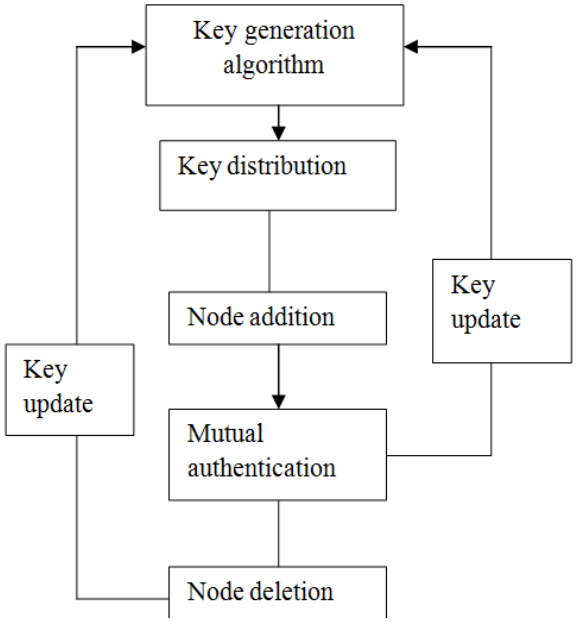

Figure1: Data flow diagram

In this method group key and the key of each node is updated whenever a node join or leave the network. Upon joining, the node is allowed to enter only if it is authenticated.

A. Group key generation using prime numbers

Group key is calculated for four quadrants using the following steps.

Steps:

1. Calculate number of nodes in the area.
2. Generate a prime number 'n', such that 'n'> number of nodes.
3. Calculate number of nodes in second quadrant.
4. Calculate next prime number 'n1', such that n1> sum of earlier prime number 'n' and number of nodes.

Similarly, calculating group key for all the regions.

B. Key generation using Euler's φ( ).

The values below the group key (GK) are assigned as a key for each node using Euler's φ( ). If GK is positive integer 'n', then $\varphi(n)$ is the number of integers 'k' such that k < n for which greatest common divisor gcd (n,k) =1.

For example, if group key is n, and number of nodes is 'm' then keys are generated as (n-1), (n-2), (n-3) etc.. till (m+1).

C. Multiplicative encryption algorithm

1. Select a plain text (PT).
2. Calculate cipher text (CT) as, CT = (key * PT) % prime number;

Where, prime number is group key of the sending node.

3. Generate PT at the receiving node as,

PT= $(key^{-1} * CT)$ % prime number.

key^{-1} is calculated using the multiplicative inverse algorithm where, $key^{-1} * key = 1$ % prime number.

V. CONCLUSION

The paper proposes a novel approach for group key management which uses prime numbers to generate group key. The paper describes a secure key management system for group that does not rely on a centralized authority for generating and distributing keys. The proposed method is simple, scalable and robust. And it reduces computation and communication.

REFERENCES

[1] Wallner, D.M., Harder, E.J. and Agee, R.C.,"Key management for multicast: issues and architectures," Internet Draft, draft-wallner-keyarch-01.txt, 1998.

[2] S. Mittra. Iolus, "A framework for scalable secure multicasting," Journal of Computer Communication Reviews, 27(4):277–288, 1997.

[3] P. Adusumilli, X. Zou, and B. Ramamurthy, "DGKD: Distributed group key distribution with authentication capability," Proceedings of 2005 IEEEWorkshop on Information Assurance and Security, West Point, NY, USA, pp. 476–481, June 2005.