IRBAS www.irbas.academyirmbr.com August 2013
International Review of Basic and Applied Sciences Vol. 1 Issue.3

Improve Quality of Service and Secure Communication in Mobile Adhoc Networks (Manets) Through Group Key Management

MUHAMMAD IMRAN KHAN KHALIL
Lecturer, Department of CS & IT
University of Engineering & Technology, Peshawar, Pakistan
Email: Imrankhalil79@gmail.com

Abstract

Mobile Adhoc networks (MANETs) is compendium of self-governing terminals, which basically interconnect and exchange information with each other and by establishing a multi-hop network for to maintain connectivity in a decentralized approach. In this research group key management approach is used, which further uses a symmetric group key for to communicate inside the cluster. Clusterhead is responsible for the generation of group key and is responsible for the communication of other nodes throughout a secure path which uses public key cryptography scheme. Encryption of messages is used for group keys to communicate inside the cluster and within the group for secure communication. In this research the results are shown through how to secure communication in MANETs through group key and clustering scheme minimizes the packet damages as compared to centralized approach. And also examine the system for proper authentication of public and private keys and evaluates the functioning of proposed methodology.

***Key Words**: Public Key Cryptography, MANETs, Group Key, Authentication, Hash tree*

Introduction

A Wireless Mobile Adhoc Network contains mobile battery operated computing devices that communicates through a wireless channel, whereas the memory space of the related computing devices and processing power rise at very fast speed. The rapid growth in Adhoc networks can be seen in various applications in commercial, educational areas and telecom sectors. Nodes communicating in wireless networks transmit without the need for any wired link. However, all mobile mechanisms are typically powered by restricted energy sources, where a continuous recharge of mobile nodes is hardly manageable. The significant method for saving energy is topology control and proper selection of the clusterhead on the basis of maximum battery power (Bose, Morin, Stojmenovic, & Urrutia, 2001).

Various groups wish to establish a same private channel to be utilized to communicate information is group key generation. Exclusively trust on central entity, two individuals don't previously exchange a same secret can be established single based upon the Diffie Hellman (DH) protocol. The general version of n-party (DH) is extended form of two-party DH protocol. Various research attempts have place in the design of the management of group key approach for the purpose of security, scalability and reliability (Kim, Perrig, & Tsudik, 2000).
Moreover, management of group key needs to find out the issues of security related to changes of membership. The amendment of membership needs to refreshment of group key. This purpose done through by updating right afterward change of member or periodic rekeying. To ensure forward and backward security is through group key change. Exchanging the group memberships frequently, various research studies started more consideration on the effectiveness of the updating group key.

GKM protocols can be generally divided into three types: distributed, decentralized and centralized (Rafaeli & Hutchision, 2003). A sole entity is active to manage the entire group and is just accountable for rekeying of group in centralized group key. Various nodes are responsible for the management of group as compared to single entity in decentralized scheme. While establishment of group key and similarly accountable for distribution and rekeying of group key in done through group members in distributed system.

In this research study, utilize the mixture of private key and public key cryptography with no central power mean decentralized approach is used. Also discuss the entire computer network topology as a group and each cluster handle as subgroup. Presume in each cluster, node can obtain information from different nodes. The complete combination of nodes is distributed in different clusters. Every cluster is managed by clusterhead. The points inside the cluster share information by using cryptography scheme symmetric key and they further shared group key to all nodes. To encrypt generated group key is used in asymmetric key cryptography, when changes in membership occur. Utilization of authentication and hash trees is done for authentication. Through this methodology, we can mitigate the communication cost of rekeying the information and computation cost of authentication when changes in membership happen. It shall remove the obligations of authority which is centralized for the establishment and for the keys distribution (Burnett & Paine, 2001).

Communication is groups are normally ensured by using symmetric key cryptography and group key distribution is done by public key cryptography scheme. In this research paper, we assumed the methodology through which communication among nodes in a cluster is done by symmetric key, and for the distribution of group key to other stakeholders of the cluster is done by asymmetric key cryptography. The verification of public keys is fixed by using authentication tree (Wenliang, Ronghua, & Peng, 2005). This removes the need of taking guarantee of authority and or by central authority for verifying the group key sender.

Literature Review

Secure communication is done through proper management of key. Almost every crypto system depends upon efficient, effective, robust and secure key management arrangement. In mobile Adhoc networks safe communication is done through by involving key sharing method among different communication groups, many times key might be broadcasted insecure paths. A structure of reliance relationship wants to establish the authentication of key possession during sharing time. Whereas a few structures are only based upon a centralized TTP, and others structures can be entirely distributed. For instance, a CA is TTP in asymmetric crypto systems, a KDC is the trusted third party is symmetric scheme, and PGP no trusted third party is supposed. In mobile Adhoc networks centralized scheme is unsuitable due to vigorous environment and transitory relation between nodes (Kim, et al., 2000).

Key sharing and settlement across vulnerable path is a great risk and deteriorate from key attacks. Previous digital envelop scheme, session key is established at one end then encrypted through algorithm of public key. After that it is distributed and mended with another side. In DH approach, information sharing groups from both ends share public data and produce a session key. Most of the improved DH methodologies have created to counter attacks namely man in the middle. In method needing a TTP, the PKC is promised for fellow nodes in distributed way, such as PGP (Burnett & Paine, 2001).
The formation of group key indicates that various parties wish to establish a same secret which is utilized to share information safely. Exclusive of depends upon a main trusted node, two points which don't before distribute a same secret now generate on the basis of Diffie Hellman protocol ("The Network Simulator ", 2008).
The LKH is a central management group key approach suggested by Wallner. Basically this scheme is rely on tree system with every member conforming to a leaf, and group originator as a base point. The system of tree shall considerably minimize the no. of broadcasted information and stowage area for group member and controller.

Every lead point distributes a key pair wise the base point with intermediary key from it root node. Therefore stable tree (binary), every member within group saves almost (d+1) keys, whereas d means tree height and n denotes no. of member in a group (Bose, et al., 2001).

Alternative scheme for the management of group key is one way function-OFT which is suggested by Sherman (Sherman & McGrew, 2003). This is based upon the structure of tree and alike to the LKH approach. Moreover, almost every key in one way function scheme are function wise depends upon to the OWH function. A user in a group yet requires for save (d+1) keys, whereas d denotes the tree height and n denotes the group members. These approaches have same complexity level which LKH approach has, however in re-keying procedure size of key material mitigates up to log n form 2log n.

TGDH is a management for group key approach suggest in (Kim, et al., 2000). The core methodology behind this scheme is to unite the efficacy of the structure of tree with the combine characteristics of Diffie Hellman protocol. The core idea of this approach is to every member supplies its contribution to group key, which is calculated as for the purpose of whole contribution of existing members. Whereas group develops novel member's distributed as factored in the group key however previous group member's distributes unaffected. When the group shortens, leaving its member's shares is eliminated from its novel key and atleast single residual node alter it shares. Entire protocols information are authenticated by the source by using RSA.

SEGK approach for group key management for mobile Adhoc networks suggested in (Bing & Dong, 2008) group key is computed by group members but in the distributed way. The core plan behind this approach is the formation of multicast tree for to enhance the efficacy in mobile Adhoc networks. Members in a group behave as coordinator in group to find out and allocate the intermediary keying to all its group members with the help of links which are active tree. Same as MS. Bousassida (Bouassida, Chrisment, & Festor, 2008) established a novel concept regarding BALADE, which is depends upon sequential model which is basically multi source, and further it obtains mobility and localization of different nodes, whereas enhancing bandwidth and energy utilization.

Proposed Scheme

The whole collection of group members in the mobile Adhoc networks is classified in to a no. of further sets which is known as clusters, and clusterhead is the leader and manager of all nodes within cluster. The format of Adhoc networks is presented below in figure 1. The manager node means clusterhead is alike with every aspect with other members of the cluster in the Adhoc networks. The public keys encrypt the messages through secure and safe path for the exchange of information among different nodes within and outside the cluster. The authentication of all public keys is done with the help of authentication and hash trees. The generation and distribution of group key to all its group members in secure path is responsibility of clusterhead. When changes materialized in membership, the regeneration and distribution of group key but in secure path is done by clusterhead. One clusterhead is selected among different clusterheads as a leader, and primary duty of this leader is distribution and generation of clusterheads. However tis approach looks same as with centralized approach, but this approach is purely works on decentralized way and we know that there is no common point of malfunction or breakage of network. Deprived of disturbing the mechanism of the whole network the whole protocol can be restarted.

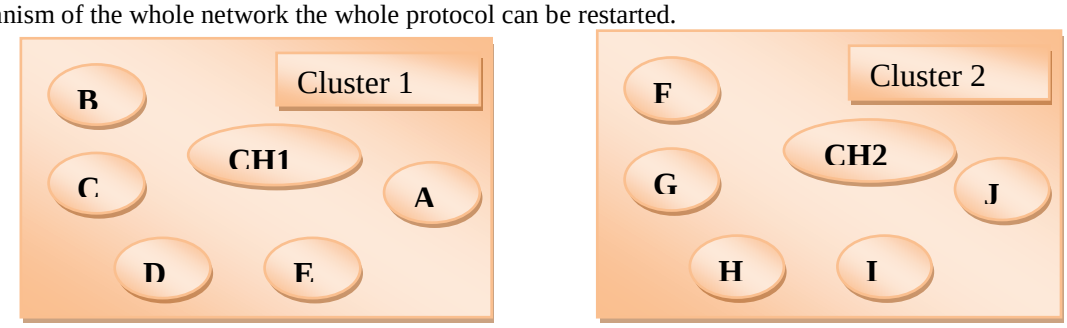

Figure 1: Scheme of clusters

Proposed Model

- Every node is allocated an exclusive integer number "ID" for the identification of node within the mobile Adhoc networks. 0 is assigned to its members and 1 is assigned to all its clusterheads.
- We suppose that, a disconnected authority which organizes the points in the mobile Adhoc networks and their related problems a proper certificate binding along the public key for verifying the member node it enter initially in the network.
- Two categories which are utilized in the cluster:
  - GK (Group Key) utilized for to encrypt the information exchanged in communication in group with the cluster.
  - PK (Public Key) used for individual members for KEK (key encrypting key), purpose of this is encryption of GK establishment when changes occur in membership.
- Protocol contains in various steps:
  - Initialization
  - Group key distribution and generation

Initialization

Phase 1: Afterward placement, the point's multicast their identification (ID) number to their nearest nodes with (Hello) message.

Phase 2: The smallest identification (ID) between entire nearest nodes are chosen as clusterhead. Updating the nodes values consequently.

Phase 3: clusterhead transmit information (message) "I am clusterhead" for to understand their member nodes.

Phase 4: The neighbor node give response with information (message) "I am member node" then cluster established in the network accordingly.

Phase 5: When node obtains multi messages from different node "I am clusterhead", then the selection criteria is on the basis of maximum signal strength.

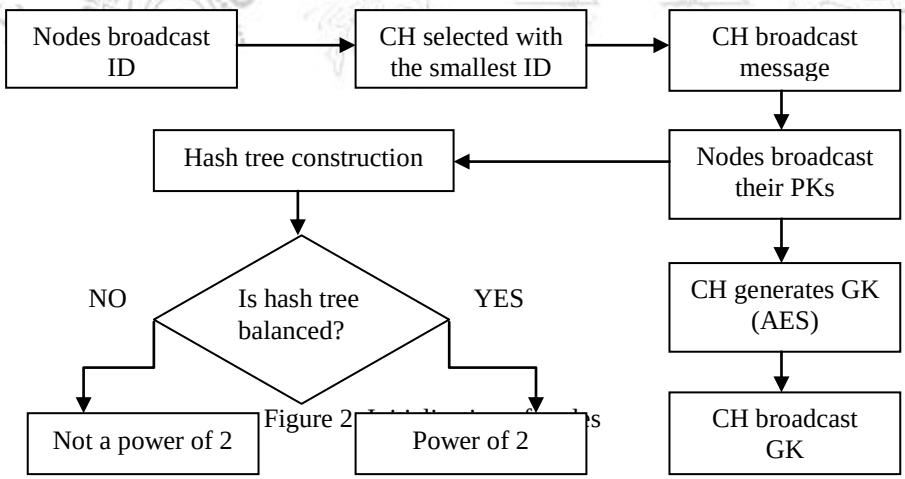

Figure 2

Group key distribution and generation

This step contains two levels:

a. Distribution and generation of group key in cluster
b. Distribution and generation of group key among clusterheads

Distribution and generation of group key in cluster

Phase 1: The clusterhead transmits public key to nearest nodes.

Phase 2: Transmission of public keys to its member along with ID's to entire nodes in clusterhead

Phase 3: The establishment of HASH tree by clusterhead with their members and the tree leaves.

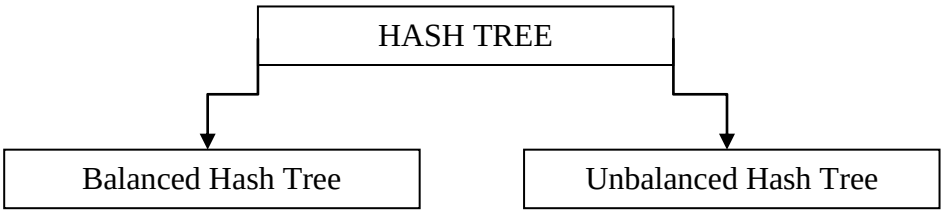

Figure 3: Authentication of Nodes

Phase 4: the root HASH number sends by clusterhead to every member's, and also transmit the intermediary HASH number to every of the points (nodes) for the purpose of authentication of public key.

Phase 5: Clusterhead produces a symmetric key with the help of advanced encryption standards (AES) and transmitting it to every node with encrypted public key with the HASH value on proper channel for root authentication.

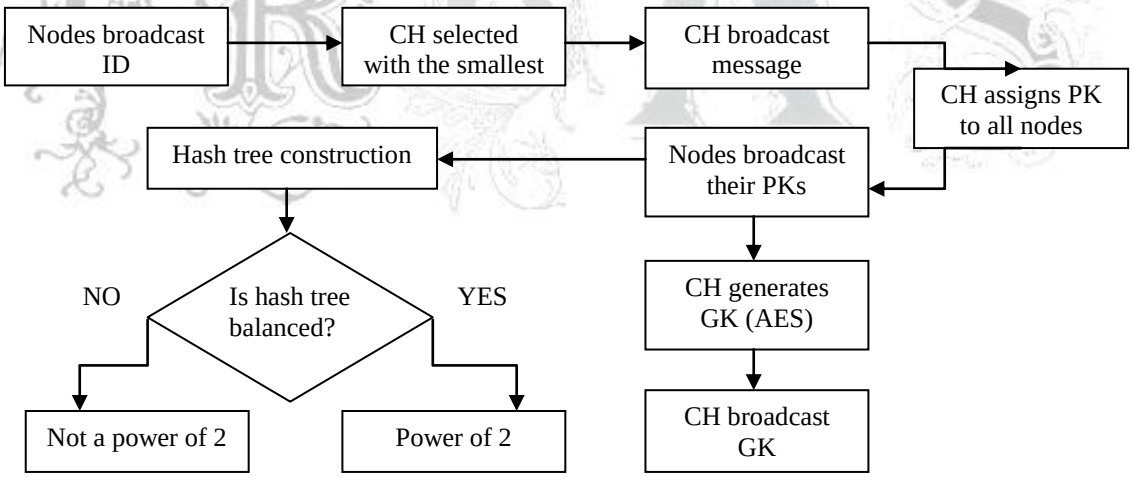

Figure 4: Distribution and generation of group key in cluster

Distribution and generation of group key among clusterheads

Phase1: Clusterheads transmit the information (message) "is any other clusterhead exists" including the identification number and public key and obtains data of clusterheads.

Phase 2: construction of HASH tree including itself by clusterheads and remaining clusterheads as leaves and find out the value of HASH root.

Phase 3: Selection of clusterhead as a leader on the basis of smallest identification number.

Phase 4: After that selected leader establishes a novel GKCH (Group key) that is further utilized for the information sharing among different clusterheads.

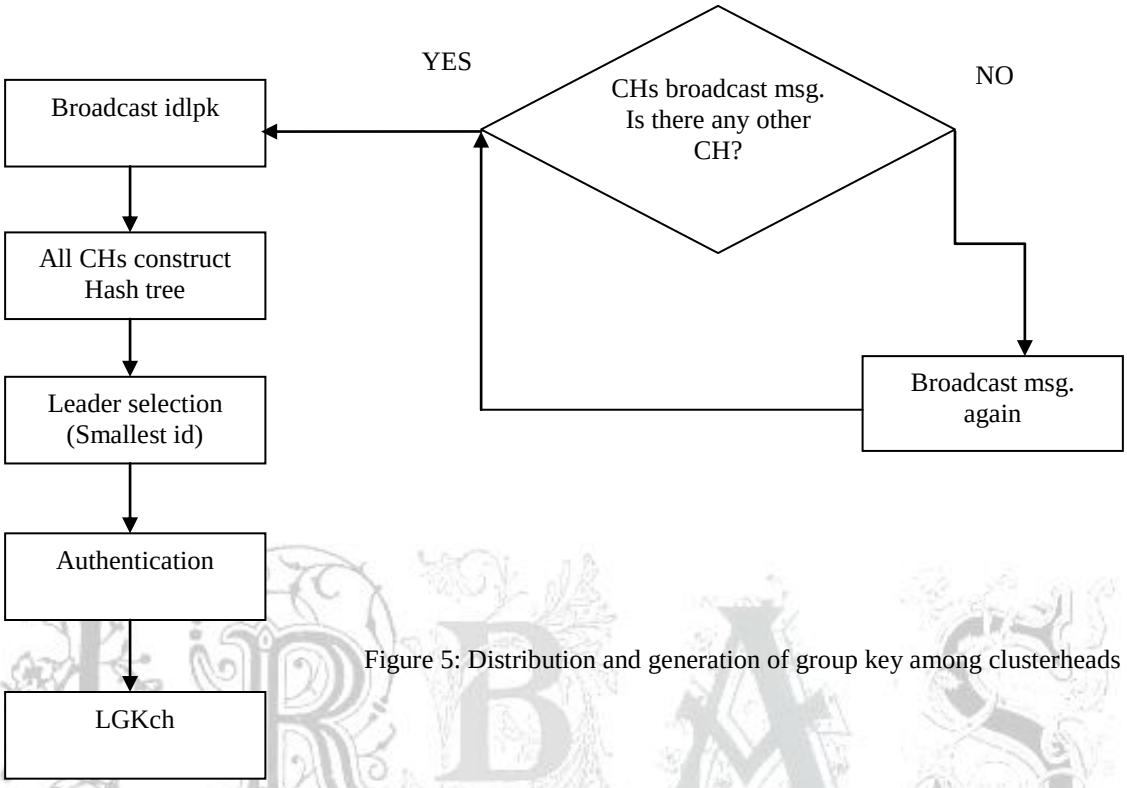

Figure 5: Distribution and generation of group key among clusterheads

Networks Dynamics

Many nodes in network are fixed. Most of the nodes can establish either a link with network or already established nodes can disconnect from the network. Every node in mobile Adhoc networks couldn't be fixed in any single location and many times they change their locations.

a. Join Member

Phase 1: Member node sends a request to nearest node after joining the network.

Phase 2: The nearest node transmit the information to clusterhead with the help of group key after obtaining the request message.

Phase 3: clusterhead transmit a response message to newly enter node after joining the cluster.

Phase 4: After that newly enter node transmit public key to clusterhead.

Phase 5: Then clusterhead reestablish the HASH tree including the newly entered member as a part of leaf of HASH tree and transmit the root value to newly entered member and then transmit to remaining nodes and encrypt it by using group key. It is also finds out the new group key and transmit to new member and then transmit it the similar to previous members again and again by encrypting the previous group key.

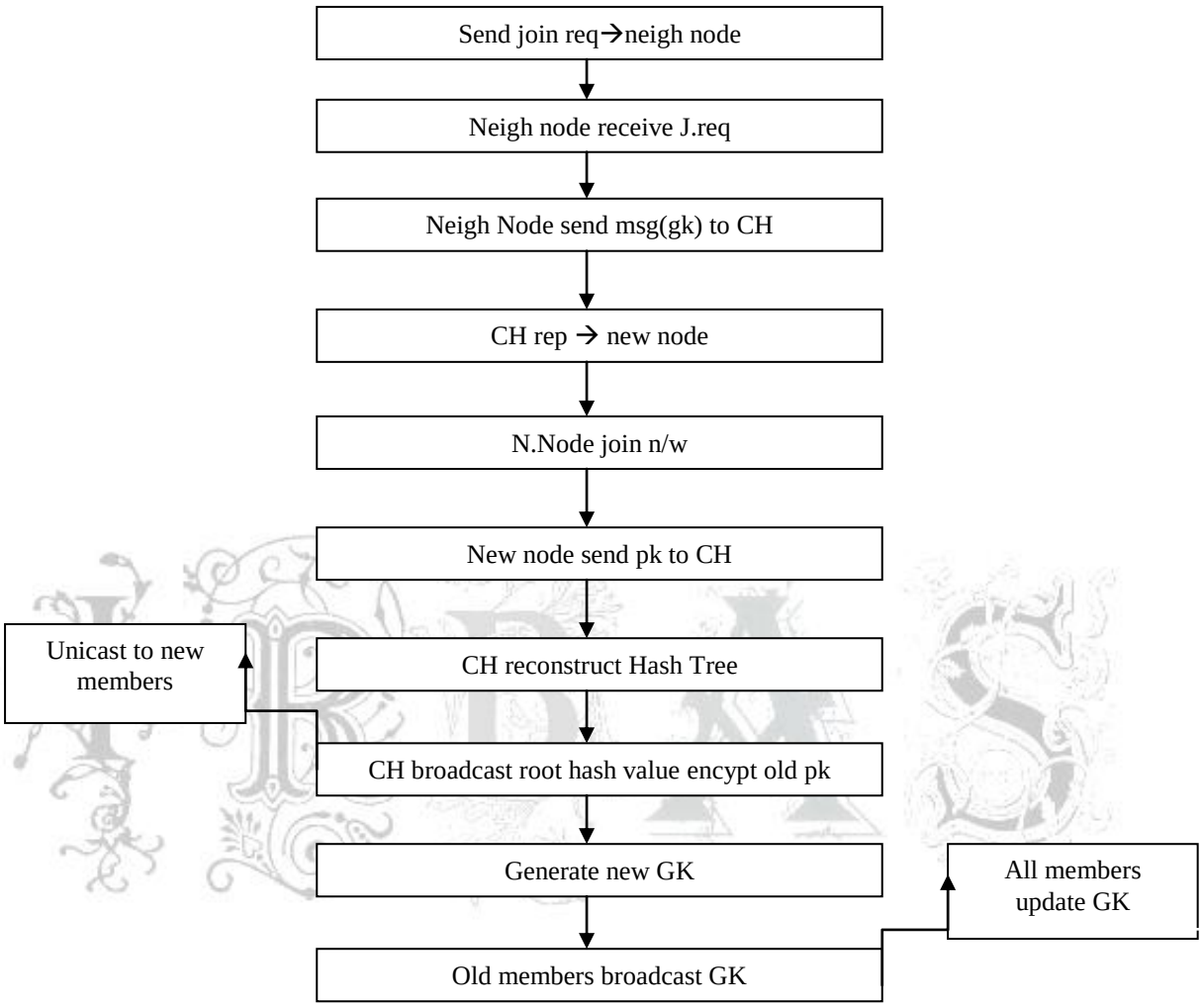

Figure 6: Joining of member

Member leaves

Phase 1: The member node notifies the clusterhead regarding disconnect or leaving the cluster.

Phase 2: After notification clusterhead gives approval for departure.

Phase 3: Clusterhead finds out a fresh group key and transmit it the other members by using unicast information (message) which is encrypted through public key, for the confirmation of disconnected member which is not able to establish the group key.

Phase 4: After that clusterhead redesign the HASH tree excluding the leaved member and get the root value, and sent this value to single member encrypted with public key.

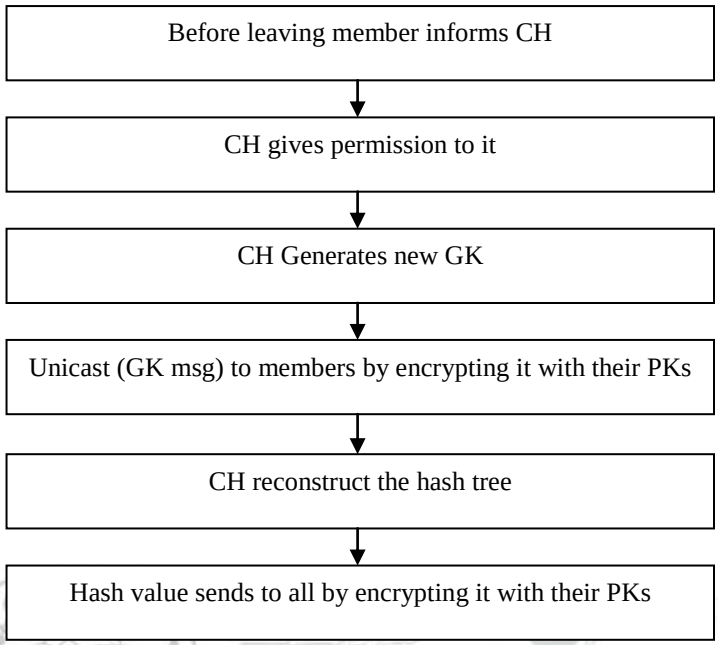

Figure 7: Members leaves

Conclusion & Future Work

In this research the proposed decentralized scheme for the management of group key which doesn't depends upon a single permission for reestablishing a novel group key and verification. It also examined the efficacy and effectiveness of the propose scheme in term of secure communication and discovered that it is reliable for different types of security attacks and facilitate the mobile Adhoc network for backward and forward secrecy.

Simulation experiments can be done with different scenarios and make it more secure by introducing private key for the communication between two nodes malicious or faculty nodes detection and detection can also be added in this research as part of future work.

References

Bing, W., & Dong, W. Y. (2008). An efficient group key management scheme for mobile Adhoc networks *Internationa Journal of Security and Networks*, *5*(3), 110-134.

Bose, P., Morin, P., Stojmenovic, I., & Urrutia, J. (2001). Routing with Guaranteed Delivery in Adhoc Wireless Networks. *International Journal of Wireless Networks*, *7*(6), 609-616.

Bouassida, M., Chrisment, I., & Festor, O. (2008). A Group Key Management in MANETs *International Journal of Network Security*, *6*(1), 67-79.

Burnett, S., & Paine, S. (2001). RSA Security's Official Guide to Cryptography. *RSA International Press*, *4*(3), 120-123.

Kim, Y., Perrig, A., & Tsudik, G. (2000). *Simple and faulttolerant key agreement for dynamic collaborative group.* Paper presented at the 7th ACM conference on computer and communication security.

The Network Simulator (2008). 2013, from http://www.isi.nsnam/ns

Rafaeli, S., & Hutchision, D. (2003). A Survey of Key Management for Secure Group Communication. *ACM Computing Surveys, 35*(3), 309-324.

Sherman, T., & McGrew, A. (2003). Key establishment in large dynamic groups using one-way function trees. *IEEE Transactions on Software Engineering, 29*(5), 444-458.

Wenliang, D., Ronghua, W., & Peng, N. (2005). An efficient scheme for authenticating public keys in sensor networks. *An International Journal of MobiHoc'05 5*(2), 223-229.