*IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*
*e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 10, Issue 4 Ver. II (July – Aug. 2015), PP 52-57*
*www.iosrjournals.org*

# Efficient and Secure Key Management Scheme for Mobile Ad Hoc Networks

M. El-Bashary[1] A. Abdelhafez[2] W. Anis[3]
*Dept. of Comm. and Electronics Ain Shams University*

***Abstract:*** *A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes that is self-organized to form an arbitrary topology with the absence of fixed infrastructure or centralized administration .In such environment security has become a main concern to provide confidentiality, authentication, integrity, availability, access control, and non-repudiation.*

*Key management is the main component in MANET security.This paper proposes an efficient and secure distributed group key management scheme. Where, nodes in the network are divided into clusters. Each cluster has a cluster head (CH) and cluster members. Cluster head is responsible for maintaining the group key. It also updates the group key whenever a member joins or leaves the cluster. There-keying process takes place within the cluster only. So the computation and communication cost will be reduced. Another level of security is considered between communicating parties belonging to different clusters.*

***Keywords:*** *Group Key Management, MANET, Clusters.*

## I. Introduction

Many of military and public safety applications based on MANET, as they can be rapidly deployed and configured. MANET suffers from dynamic topology, infrastructure-less, resources constraints, scalability, limited power, and limited physical security. Secure communications is needed in such environment.

Multicast transmission is an efficient communication mechanism for group oriented applications (such as video conferencing, video streaming, e-learning...) to save network resources.So group key management is the most appropriate scheme in case of combination between MANET and multicast.

A group key should be shared among all members (nodes) in the group in order to multicast information. Encryption of information by group key lets the authorized users only that have the same group key to decrypt the information. But according to MANET characteristic, members of a group may be changed. If a new member joins the group, a new group key must be generated and distributed to all group members including the new member. This process prevents the new member to access the former information exchanged through the group, which is known as "Forward Security". The same process is taken when a member leaves the group as it has no rights to access the information anymore which is known as "Backward Security".

MANET can be exposed mainly to two types of attacks: passive attacks and active attacks. A passive attack obtains data exchanged in the network without affecting the operation of the communication, while an active attack involves information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping, traffic analysis and traffic monitoring. Examples of active attacks are: jamming, impersonating, modification, denial of service (DOS) and message replay.

The remainder of this paper is structured as follows: in Section 2; Related Work is presented, in Section 3;Proposed Scheme will be explained; Security Analysis of Proposed Solution will be discussed in Section 4. Finally, we conclude the presented work in Section 5.

## II. Related Work

Group key management protocols can be classified into centralized, decentralized, and distributed group key management.

In centralized group key management protocols there is a group key server (KS) which is responsible for group key distribution and updating. The most familiar scheme is the Logical Key Hierarchy (LKH) [1]. LKH is based on the tree structure where each user represents a leaf and the group initiator as the root node. The tree structure reduces the number of broadcast messages and storage space for both the group controller and group members. Each leaf node shares a pairwise key with the root node as well as a set of intermediate keys from it to the root. One Way Function (OFT) is another centralized group key management scheme that is similar to LKH [2]. However, it proposes different ways to reduce communication overhead, and computational cost.

In decentralized group key management protocols the group is divided into subgroups. Each subgroup shares a local session key managed by a local controller, thus attenuating the "1 affects n" phenomenon. When a member joins or leaves the group, only the concerned sub-group will renew its local key. IOLUS [3] is a

decentralized scheme, where all members are arranged into subgroup in hierarchy to constitute a virtual group. Each cluster or sub-group of the multicast group shares and manages a local traffic encryption key (TEK), requiring several decryption and re-encryption operations of the multicast flow, when it passes from a sub-group to another.

DEP [4] is another scheme that uses only one TEK for all clusters in the group. It hierarchically divides the multicast group into sub-groups, each of them being managed by a sub-group manager. The managers do not need to decrypt the multicast flow sent by the source.

The Enhanced BAAL protocol [5] is based on the combination of the BAAL protocol which is a group key management protocol in wired networks, and the dynamic support offered by the Adaptive Key Management Protocol (AKMP) protocol [6]. Authentication and key generation are achieved via threshold cryptography [7] as shown in figure (1). Each entity of the group holds a public and a private key, generated by the server nodes of the threshold cryptography. The principal actors of this architecture are the global controller (GC), the local controllers (LCs) and the members of the multicast group. The GC is the source of the multicast group, and is responsible for the generation, distribution and periodic renewal of the TEK. The GC combines the contribution of threshold cryptography servers to generate the TEK, and then distributes it to all group members. LC manages a local traffic encryption key, and is responsible for forwarding the multicast flow sent by the source to all its local members. LC is a member of the multicast tree, forming a subgroup with its local members. This protocol attenuates the "1 affects n" phenomenon. However, the intermediate operations of data encryption and decryption remain very constraining in an ad hoc environment, with limited resources of storage and computing power.

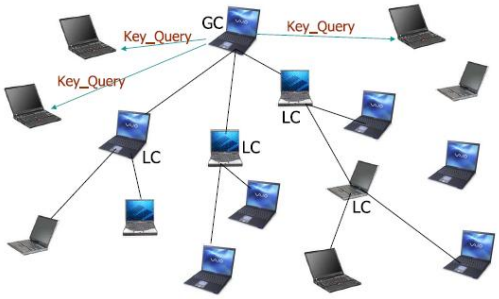


**Figure (1): The group key generation and distribution in Enhanced BAAL.**

In distributed group key management protocols, and sometimes called key agreement, all members in the group cooperate to generate and distribute the traffic encryption key (TEK) for secure communications between them. The need for a trusted central authority is eliminated. All group members have the same responsibility, capability and are equally trusted. Whenever a member joins or leaves the group, any member can initiate the rekeying process. There are some other forms of key management schemes based on this approach such as Burmester and Desmedt (B-D) scheme [8], and BALADE [9].

In BALADE the multicast group is divided dynamically into clusters as shown in figure (2). Each cluster is managed by a local controller LC which shares with its local members a local cluster key $KEK_{CSG}$. The multicast flow is encrypted by the source with TEK and sent in multicast to all the group members. The source of the group and the local controllers form a multicast group called Group of Local Controllers (GLC) and share beforehand a session key called $KEK_{CCL}$. Each new local controller has to join this group and receive the session key $KEK_{CCL}$ from the source of the group, encrypted with its public key. The multicast source sends the TEK to the group of the local controllers, encrypted with $KEK_{CCL}$. The local controllers forward the TEK to their local members, encrypted with their respective local cluster key.

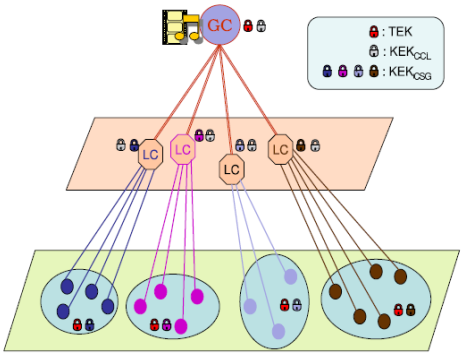


**Figure (2): The group key generation and distribution in BALADE.**

The centralized group key management protocols are easier to implement, but it is clearly not scalable since it suffers from the "1 affects n" phenomenon. The KS is considered being a bottleneck and a single point of failure. The decentralized group key management protocols need less bandwidth for key updating process. While the distributed group key management protocols are complicated and less scalable, but may be is the most appropriate approach for MANET as it eliminates the bottleneck and the single point of failure problems as well as "1 affects n" phenomenon.

## III. Proposed Scheme

The proposed scheme is based on distributed group key management approach where no central authority exists. The users themselves collaborate to generate a group key through simple computations. In large and high mobility ad hoc networks, it is not possible to use a single group key for the entire network because of the cost of computation and communication for rekeying. Thus the network is divided into clusters. Each cluster contains a cluster head CH, and number of cluster members.

### 3.1. Cluster Formation

A "Hello" message is broadcasted from every node to its one hop neighbors carrying its ID, public key, location, weight in terms of communication power, energy, and processing capabilities. The nodes in a group are divided into clusters according to their locations. Each cluster will elect one of the nodes to be cluster head (CH) according to its weight, while the other nodes are cluster members. The cluster members have one hop to the CH. Users are in a flat network topology, and the key management scheme is centralized within the cluster. The CH is responsible for cluster management, and group key distribution and rekeying. The cluster formation is shown in figure (3).

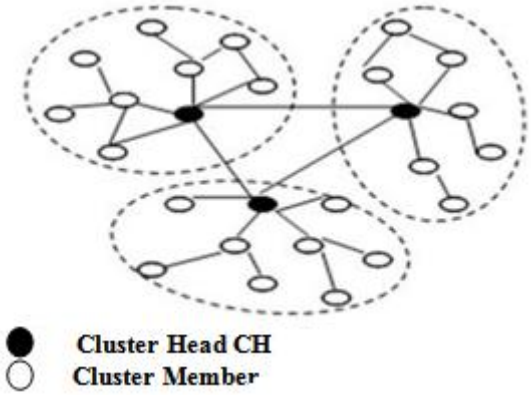


**Figure (3): The Cluster Model in MANET**

### 3.2. Cluster Head (CH) selection

For CH selection, node's mobility, battery power and behavior must be taken into account. The following factors are considered for clustering:

- Each CH is capable to support maximum 'x' number of nodes (a pre-defined value) efficiently. If a CH is trying to serve more than 'x' nodes, system's efficiency suffers.
- Mobility is an important factor in selecting the CH as it is responsible for preserving the structure of a group as much as possible when nodes move. Moving CH results in detachment of nodes from cluster and also increases the probability of nodes' compromised. Mobility of a node is denoted by 'M' and can be measured as:

$$\boldsymbol{M = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}}$$

Where, (Xt, Yt) and (Xt-1, Yt-1) are the coordinates of a node at time t and t-1.

- 'Battery power' (B) is another important factor to decide a CH, as it consumes more battery power than any other node. Then node with maximum battery power should be elected as CH.
- Another important factor is the 'behavior of the elected node. Security of a group is totally depends on CH, as it monitors the nodes' activities and assigns them a Trust Level (T) on the basis of their behavior.
- Finally, CH selection is based on its weight (W), which can be defined as:

$$W = w_0 M + w_1 B + w_2 T$$

### 3.3. Group Key Generation and Distribution

Each node carries a valid certificate from offline configuration before entering the network. So every node has an ID, a public key and a private key. The proposed protocol assumes three types of keys in the network:

- **Cluster Group key $K_c$:**

The cluster head CH generates a group key to share secure traffic between CH and its members. It needs to be refreshed whenever a new node joins or leave the cluster. CH is responsible for generating the group key using public keys of all cluster members as follows:

$$K_c = (\beta)^{P_1+P_2+\cdots P_n+k_{CH}} \bmod p\, S$$

Where,
β:primitiverootofa prime number p,
$k_{CH}$: secret key of cluster head,
$P_1, P_2 \ldots P_{n:}$ public keys of nodes within the cluster,
p: prime number,
S: secret random value.
The $K_c$ is encrypted by public key of each cluster member node and distributed on unicast basis.

- **Cluster Head Group key $K_{CH}$:**

Cluster Head Group key $K_{CH}$ is generated in a distributed fashion between cluster heads in the network. Cluster heads CHs of all clusters participate to generate a group key $K_{ch}$ using Group Diffie-Hellman (GDH) protocol. It needs to be refreshed whenever a new CH joins or leave the network. $K_{ch}$ is used for securing the exchange of session key $K_s$ between source and destination nodes in different clusters.

- **Session Key $K_s$:**

Session Key $K_s$ is mainly used for securing the traffic flow between any two communicating parties in different clusters in the network. This key is generated every communication session. The source node generates a secret key for every communication session $K_s$. Then $K_s$ is sent to the destination node(s) in a multicast basis, encrypted by the following keys; cluster key of the source cluster $K_{cs}$ between the source node and its cluster head, $K_{ch}$ between cluster heads of both source and destination nodes, and finally cluster key of the destination cluster $K_{cd}$ between cluster head of the destination and the destination node. Once $K_s$ is decrypted, the communication flow between source and destination can be exchanged securely. No encryption and decryption processes are needed between source and destination.

### 3.4. Joining of a New Node

Whenever, a new node wants to join a cluster, it sends a request to CH. This request might be captured by a malicious node showing as CH to new node. Similarly, a malicious node can also send a request to CH to join the cluster. Therefore, it is necessary for both CH as well as new node to authenticate each other. Upon successfully mutual authentication, a node can join the group and share a key with CH in a secure manner. A new node and CH can authenticate each other using challenge-response protocol. New node sends a challenge to CH and CH provides a valid response. After successful authenticating to CH, new node can follow the following steps to join the cluster.

- The new node sends "Hello" message to the CH containing its ID, location and public key.
- CH calculates a new group key based on the public key of the new joining node.
- CH will send the new group key in a multicast basis to existing nodes encrypted by the old group key.
- CH will send the new group key in a unicast basis to the new node encrypted by its public key.

In other hand, whenever a new cluster head joins, it broadcasts “Hello” message to neighbor cluster heads. One of the neighbor cluster heads initiates the refresh to generate a new $K_{CH}$.
By this way, the new node has not any information about the old group key maintaining backward secrecy.

### 3.5. Leaving of an Existing Node

When an existing node leaves the cluster, the following steps are followed:

- The leaving node sends "Leave" message to the CH containing its ID.
- CH calculates a new group key excluding the public key of the leaving node.
- CH will send the new group key in a unicast basis to the existing nodes encrypted by their public keys.

In other hand, whenever a cluster head leaves, it broadcasts a "leave" message to neighbor cluster heads. One of the neighbor cluster heads initiates the refresh to generate a new $K_{CH}$. The same algorithm for election a new cluster head will take place.
By this way, the leaving node or cluster head will not have any information about the new group key maintaining forward secrecy.

## IV. Security Analysis of Proposed Solution

In this section, the security analysis is discussed of proposed key management system against different attacks.

### 4.1. Backward Secrecy

When a node leaves the network, it should not be able decrypt the future encrypted traffic. In proposed key management scheme, whenever a node leaves the group, CH regenerates new group key and distribute it in the group. On the other hand, when a CH leaves the network, a new CH generates group key for the group. While the session key $K_s$ is generated every communication session. This ensures that keys are updated and backward secrecy is maintained in network.

### 4.2. Forward Secrecy

Forward secrecy says that when a new node joins the network, it should not be able to decrypt the past encrypted traffic. On joining of new node, CH generates new group key and sends to members of group encrypted with old group key and unicasts to new node encrypted with key shared between CH and new node, ensuring forward secrecy.

### 4.3. Authentication

In the proposed key management system, both new node and CH authentic ate each other mutually at the time of network joining. After successful mutual authentication, node can join the network. Also when a new cluster head joins, it mutually authenticate with the neighbor cluster head.

### 4.4. Man in the Middle Attack

Man in the Middle attack is an active attack in which an attacker takes place between two communicating parties, for instance nodes A and B. Attacker splits the connection into two connections, one between node A and attacker and second, between attacker and second node B. Two nodes A and B think that they are communicating with each other, while they communicate with attacker in between them. In the proposed scheme, both new node and CH authenticate each other using challenge-response protocol. Hence, it is not vulnerable to Man in the Middle attack.

## V. Conclusion

In this paper, it has been shown the characteristics and the challenges of the MANETs environment. The different approaches of key management protocols in MANET networks are presented. A distributed group key management scheme is proposed for mobile ad hoc network in this paper. In the proposed scheme, an ad hoc network is divided into clusters. Each cluster has a cluster head and maximum number of cluster members, so the "1 affects n" phenomenon is avoided. The proposed scheme needs a mutual authentication between new join cluster member and the cluster head. It achieves forward and backward secrecy whenever any cluster head or cluster member join or leave the cluster. A single secret key between source and destination node(s) are needed, without multiple encryption and decryption operations.

## References

[1]. Wallner, D.M., Harder, E.J. and Agee, R.C. (1998) "Key management for multicast: issues and architectures", Internet Draft, draft-wallner-key-arch-01.txt.
[2]. Sherman, A.T. and McGrew, D.A. (2003) "Key establishment in large dynamic groups using one-way function trees", IEEE Transactions on Software Engineering, Vol. 29, No. 5, pp.444– 458.
[3]. S. Mittra. Iolus: "A framework for scalable secure multicasting," Journal of Computer Communication Reviews, 27(4):277–288, 1997.
[4]. L. R. Dondeti, S. Mukherjee, and A. Samal, "Scalable secure one-to-many group communication using dual encryption," Computer Communication vol. 23, no. 17, pp. 1681-1701, 2000.
[5]. M. S. Bouassida, I. Chrisment, and O. Festor, "An enhanced hybrid key management protocol for secure multicast in Ad Hoc networks," in Networking 2004, Third International IFIP TC6 Networking Conference, LNCS 3042, pp. 725-742, Springer, May 2004.
[6]. H. Bettahar, A. Bouabdallah, and Y. Challal, "An adaptive key management protocol for secure multicast," in 11th International Conference on Computer Communications and Networks ICCCN, Florida USA, Oct. 2002.
[7]. L. Zhou and J. Haas, "Securing Ad Hoc networks, "IEEE Network, vol. 13, no. 6, pp. 24-30, 1999. M. Burmester and Y. Desmedt. "A secure and efficient conference key distribution system" In Advances in Cryptology EUROCRYPT, 1994.
[8]. M.S. Bouassida, I. Chrisment, and O. Festor. Group Key Management in MANETs. International Journal of Network Security IJNS, 2006.

[9]. G. Chaddoud, I. Chrisment, and A. Shaff, "Dynamic Group Communication Security", 6th IEEE Symposium on computers and communication, 2001.
[10]. Ayman El-Sayed, "A new Hierarchical Group Key Management based on Clustering Scheme for Mobile Ad Hoc Networks", International Journal of Advanced Computer Science and Applications. Vol. 5, No. 4, 2014.
[11]. D.S.Dawoud, S.H.Mneney, Farhad Aghdasi, Peter Dawoud, "An Efficient Hierarchical Group Key ManagementProtocol for Mobile Ad–Hoc Networks", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference, vol., no., pp.619,623, 2009.
[12]. Kamal Kumar Chauhan, Amit Kumar Singh Sanger, "Securing Mobile Ad hoc Networks: Key Management and Routing", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
[13]. W. Diffie and M.E. Hellman,"New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.
[14]. L. Lazos and R. Poovendram, "Energy-aware secure multicast communication in Ad Hoc networks using geographical location information," in IEEE Inter-national Conference on Acoustics Speech and SignalProcessing, pp. 201-204, 2003.