International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.169-182
http://dx.doi.org/10.14257/ijsia.2014.8.1.16

Security Assessment for Key Management in Mobile Ad Hoc Networks

Reham Abdellatif Abouhogail

Electrical Quantities Metrology Dept
National Institute of standards
Cairo, Egypt
rehlatif@yahoo.com, rehamabdellatif@ymail.com

Abstract

A mobile ad hoc network (MANET) is a kind of wireless communication system that doesn't have base stations or routers. The wireless connections can be a standard Wi-Fi connection or satellite, or another medium such as a cellular transmission. Specific applications like military or public emergency require secure group communication in ad hoc environments. Good Key management is very important to get protection in any communication system. This paper presents most problems of securing key management in ad hoc networks. It presents a survey of different types of key management protocols in wired networks and in ad hoc networks. It presents the most common kinds of attacks in ad hoc networks. A new efficient approach is proposed. It is based on dividing the members into clusters. This scheme assumes a maximum allowed number of members in each cluster. This reduces the required number of encryption and decryption operations for each join operation in the cluster. This is most suitable for Mobile Ad hoc Networks.

Keywords: *Wireless connections; MANETs; Security; Key management*

1. Introduction

A MANET is a communication Network characterized by the absence of any fixed infrastructure that does not have base stations or routers. Each mobile node acts as a router on the internet. A MANET system is formed spontaneously with the participating nodes without any preplanning. The system must adapt itself to the dynamics and the mobility of the nodes. In the last decade we have a spreading in the ad hoc networks. In parallel, we saw a development of multicast services. Multicast communication is an efficient mechanism for group communication applications. It has several applications like: distance learning, video conference, pay per view TV and financial stock quote distribution. The main advantage of multicast communication is to save network resources. By applying multicast services with ad hoc network, we'll get challenges in the security field. Several applications have to be secured in ad hoc environments for example group communications in a battle field in military applications, spontaneous collaborative activities, emergency communications and sensing applications. Because of wireless connections in MANETs, MANETs is vulnerable to many different types of attacks like: modification, denial of service, listening, traffic diversion and repudiation. So, assuring a certain level of security in these networks is a requirement.

To satisfy authentication, data integrity, data confidentiality and prevention of attacks, key management protocol must be established. The key management protocol is responsible for:

ISSN: 1738-9976 IJSIA

1. The generation of the traffic encryption key (TEK).
2. The distribution of the TEK.
3. Updating this key.

The traffic encryption key is used to satisfy the authenticity because it's used by the sender to encrypt multicast data and by the receivers to decrypt it. Key management schemes always concentrate on improving security and reducing the memory storage of keys.

In a MANET, if a message is sent out through a general tunnel without encryption, it may suffer from malicious attacks. Key management schemes usually focus on improving security and reducing the memory storage of keys. We have two common types of key management. The first one is Clustering [1, 2] and the second one is hierarchical trees [3, 4]. Clustering scheme idea is to divide the multicast group into subgroups. Each subgroup is managed by a local controller (LC), which is responsible for local key management within its cluster. Thus, after join or leave operations, only members within the concerned cluster are affected by the rekeying process, and the dynamic feature of the system doesn't affect the other clusters of the group. The advantages of clustering are that rekeying can be done quickly. However clustering brings new challenges in MANETs such as synchronization and excessive communication overhead to maintain clusters. In this paper, Section 2 presents the problems that key management in ad hoc networks face. Key management protocols in wired networks are presented in Section 3. Many types of security attacks in ad hoc networks are presented in Section 4. A survey of key management protocols in ad hoc network is presented in Section 5. Section 6 describes new proposed key management protocol suitable for MANETs. Finally, Section 7 concludes the paper.

2. Problems of Securing Key Management in Ad Hoc Networks

There are many problems we must solve to satisfy a suitable level of security in ad hoc networks. This is because the difficult nature of this system. The difficult nature of this system can be concluded in the following constraints:

1. No Infrastructure: this feature is considered one of the main features of ad hoc network. There is no any pre-deployed infrastructure or any centralized entity. So, key management based on trusted centralized authority is impossible. This is because the difficulty of marinating an entity and if it happened this point will be a point of weakness, which is vulnerable to attacks.

2. Mobility and dynamism: the topology of the network changes continuously and unpredictably. Thus, the key management protocol has to be suitable for this feature.

3. Wireless communication: the wireless communication is more susceptible to two types of attacks Passive attacks like: sniffing and active attacks like: message replay and message alteration.

4. Energy Consumption and bandwidth: in ad hoc networks, the used devices are limited in energy, bandwidth, CPU and memory capacities.

5. Uncontrolled size: many changing in the number of members in ad hoc networks. Thus, a key management system has a load to be adaptive to these changes.

Before presenting the key management in ad hoc networks, we must present key management in wired networks. Many key management protocols are proposed for

securing multicast communications in wired networks. In the next section, three principles that the proposed protocols in wired networks are relied on will be presented.

3. Key Management Protocols in Wired Networks

The classification of key distribution protocols in multicast wired networks is as follows:

1. Centralized Group Key management Protocols

In the centralized key management, a single entity is responsible for generation, distribution and rekeying of the keys. This type suffers from the "1 affects n" phenomenon. This entity is considered as a bottleneck. Some examples of centralized group key protocols are: Logical Key Hierarchy [3] and [4], centralized flat table (CFT) [5] and One-way Function Tree (OFT) [6]

2. Decentralized Key Management Protocols

This type divides the group members into subgroups. Each group has a local session key and has a local controller manages this group. So the management of a large group is divided among subgroup managers. This type of protocols is divided into two categories. The first one has a different key for each cluster or subgroup. The second category has a single key for all subgroups. So the first type suffers from several decryption and re-encryption operations during the multicast communication from subgroup to another. An example of this type is IOLUS [5]. While the second one suffers from more key encryption keys (KEKs). This is because the mangers of the group are not members in the subgroups. So they don't need to decrypt the multicast flow sent to it. An example of this type is DEP [6]. These two types of protocols are not suitable for ad hoc network. They are not suitable to the dynamics of the ad hoc network.

3. Distributed Key Management Protocols

In this type, there is no certain entity works as a manager. All the members work to generate the group key. So this type sometimes called key agreement approach. This type minimizes the problem of 1 affects n phenomenon. But this type suffers from more encryptions and decryptions processes between subgroup managers. Some examples of this are [7] and [8].

4. Security Attacks in Ad Hoc Networks

The attacks in MANET can be classified into two types: 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.

Attacks can also be classified into internal attacks and external attacks. External attacks are carried out by nodes that don't belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal nodes know valuable and secret information, and posses privileged access rights.

Attacks can also be classified according to network protocol layers. In the following, we will present some attacks according to the protocol layers.

4.1. Physical Layer Attacks

Most of the wireless communications use the RF spectrum. A radio jammed can be easily jammed or interfered. This causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong to disturb the signal. Signals in wireless medium communication can be eavesdropped. Eavesdropping is intercepting and reading of messages and conversations by unintended receivers.

4.2. Network Layer Attack

The connectivity between nodes is done in this layer. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. Also, the packets could be forwarded to a nonexistent path and get lost. In the following, we will introduce the two most famous types of attacks work with this strategy. They are the wormhole attack and the blackhole attack.

4.2.1. Wormhole Attack

An attacker records packets at one location in the network and tunnels them to another location. The tunnel between two colluding attackers is referred to as a wormhole [9]. Sure, the routing is changed when routing control messages are tunneled. The wormhole attack is considered one of the most severe threats to MANET.

4.2.2. Blackhole Attack:

It’s also called a packet drop attack. This happens when a router that is supposed to relay packets discards them. This type of attack is very hard to prevent or detect. The malicious router can also accomplish this attack selectively. For example, by dropping packets for a particular network destination at a certain time of the day, or dropping a packet every number of packets or every certain time seconds, or a randomly selected portion of the packets. This is rather called a gray hole attack [10]. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly.

Through a Mobile Ad-Hoc Network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised then deceive the other hosts in the network [11].

4.3. Transport Layer Attack

The end-to-end reliable delivery of packets is done through the transport layer. As the TCP protocols in the Internet, the mobile node is vulnerable to SYN flooding attack. But, a MANET has a higher channel error rate when compared with wired networks.

- **SYN Flooding Attack:** the SYN flooding attack is a type of a denial of service attack. In this type of attack, the attacker sends multiple times of requests to establish a connection with a router. Then, the attacker doesn't complete the connection. For example, the malicious client doesn't send the expected acknowledgement. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but the attacker will establish large numbers of half-open connections with the server until

no new connections can be made resulting in a denial of service to legitimate traffic [12].

- **Session hijacking** Session hijacking, also known as TCP session hijacking is a method of taking over a web user session by secretly obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and does anything the user is authorized to do on the network. The session ID is normally stored within a cookie or URL.

4.4. Application Layer Attacks

The application layer contains user data, and it normally supports many protocols such as HTTP, SMTP, FTP. Application layer attacks can be mobile viruses, worm attacks and repudiation attacks.

- **Virus and worm attacks:** malicious programs are widely spread in the network. Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your wireless network. there are a number of techniques by which a worm can discover new machines to exploit. One example is IP address scanning, which is used by Internet worms. This technique consists of generating probe packets to a vulnerable UDP/TCP port at many different IP addresses. Hosts that are hit by the scan respond, receive a copy of the worm and hence get infected. The Code Red worm [13] is one of the scanning worms.

As we mentioned before, key management protocols are established to manage the key generation, storage, distribution, updating, revocation and certificate service. Target of attackers is to disclose the cryptographic key at the local host or through the key distribution process. Because MANET hasn't a central entity, it is more vulnerable to key management attacks. Like for example, the man in the middle attack. The next section presents the principle approaches related to the group key management protocols in MANETs environments.

5. Key Management Protocols in Ad Hoc Networks

The group key management in wired network is different from it in wireless network. In this section we present several types of key management in ad hoc network. We divide these types into three main categories. These three categories are of the same names as the names of the main three categories of key management protocols in wired network. So we will divide this section into three subsections. We will present in the three subsections some of the different techniques that are used to manipulate the special specifics of the ad hoc network system.

5.1. Centralized Category

In this category, the management is mainly carried by one central entity in the network. Kaya *et al.*, [14] provided a certification service. The certification service is presented to ensure access control. Only entities of valid certificate are able to access the multicast flow. A trusted third party (TTP) gives a signed security certificate to the nodes who wanting to join the group. Excluded nodes have revoked certificates. This is done by sending periodically a signed certificate revocation list. So the group members store this list, and make a check for each new member wants to join the group. This feature reduces the communication cost and

complexity in MANET. The new nodes select the nearer tree to join. By using the GPS (Global Positioning System) information they can know the nearest and suitable tree. The new member sends a join request. The join request is sent through a limited period of time. This limited time is called TTL (Time to Live). This feature builds a multicast tree with short paths, which makes the key distribution is more easy and optimized. To counter replay attack the protocol is carried out by TESLA [15] protocol.

GKMPAN [16] protocol depends on multiple rekeying phases. We can conclude the phases of this protocol into four phases:

- The first phase (The key redistribution phase): each group member obtains a subset I_u of m keys out of the pool of l keys. These keys are used as KEKs (key encryption keys).
- The second phase (Authenticated node revocation): when the key server revokes a node, it broadcasts a revocation message to the network. This message contains the identifier of the revoked node, and the non compromised key that is possessed by the maximum number of remaining nodes in the network.
- The third phase (Secure group key distribution): in this phase the server generates and distributes a new group key. When a node is compromised and is revoked by the key server, the key server determines the identifier of the non compromised KEK, shared with the maximum number of members. Then the server sends a multicast message authenticated by TESLA [15]. This message contains the new group key encrypted with the non compromised KEK. Group members, who can't get the new group key, will receive it from their neighbors, encrypted with other non-compromised KEKs. The group nodes send the new group key to their neighbors in a hop by hop way.
- The fourth phase (Key Update): the group members update their KEK's after receiving the new group key. The compromised KEKs k_i*'s* are also updated by the remaining members using these keys, using a non compromised keys k_n*'s*, using the pseudo random function f as follows:

$$k_i' = f_{kn}(k_i) \quad (1)$$

Lazos *et al.*, [17] proposed a new approach taking into account the energy efficiency. He tried to improve the key distribution of LKH [18] by inserting the energy consumption into consideration. Lazos *et al.*, used the geographical localization of the group members. Members which are geographically close to each other can potentially be reached by a broadcast message, or can use the same path to receive the multicast data. K-means clustering algorithm is used to form groups. The key distribution process which is based on K-means algorithm is composed of the following steps:

1. Assign all the group members in one global cluster.
2. Divide each cluster into 2 sub-clusters using the k-means algorithm.
3. Use a refinement procedure to balance the number of members per cluster.
4. Iterate step 2 and 3 until clusters of two or one points have been created.
5. Merge clusters with only one member.
6. Map the cluster hierarchy into the LKH tree.

5.2. Distributed Category

Group key management in distributed approach has no single point of failure. All the multicast group members cooperate to ensure secure multicast communications. Kong *et al.*, propose a distributed Multicast Group Security Architecture for Mobile Ad Hoc Networks [19]. He distributes the group key management to distributed mobile nodes. In each k-hop neighborhood, a clusterhead is dynamically elected. The key distribution process is based on the following two phases:

First phase assumes that there are certain candidate Group Controller Key Server (GCKS) nodes. They are special nodes with relatively large computational resource and high tamper resistance capability. Between all N certified network member nodes, η.N of them are capable of being GCKS nodes. It's called a fully distributed cluster formation phase: In this phase, the candidate GCKS nodes that don't belong to any cluster can start a cluster formation by broadcasting a cluster head claim packet up to *k* hop away to claim itself as a cluster head. The TTL (Time-to-live) parameter determines the number of hopes the claim packet can hop. For each hop the TTL is decreased by one until the TTL field become zero, and the packet dropped. All neighbor nodes, which received this claim packet become member of the cluster and give up their right to be a cluster head. In case of multiple broadcasts concurrently occur, the node with least TTL value and lower ID wins the competition to be cluster head. The second phase is called: fully distributed cluster maintenance phase. In this phase the cluster head sends a cluster head claim packet to all its cluster members periodically every t_{head}. If a cluster member node does not receive a cluster head claim packet from its cluster head for a timeout; which $t_{time\ out}$= 3* t_{head} (Note: the coefficient 3 can be adapted upon measuring local channel error rate traffic and contention ratio), so the node doesn't belong to its current cluster. This node must join another cluster when it receives a cluster head claim packet from other cluster heads or it may declare itself as a cluster head after a random waiting time.

Mawloud et al. [20] proposed a fully distributed trust model. The scheme based on a trust graph for mobile ad hoc networks. In this system, users' public/private keys are created by the users themselves, and key authentication is performed via chains of public key certificates in the graph of trust. Instead of storing certificates in centralized certificate repositories, the system stores certificates by nodes themselves. The main contribution of this approach is the inclusion of a threshold scheme within the graph of trust. The private shares are used to sign certificates instead of using private keys. This approach includes four basic operations:

1. Initialization Phase: a private share S_i of the system's private key K_{system}^{-1} is configured to each member *i* in the system using a (*k*,*n*) threshold cryptography scheme, where *n* is the number of members in the network, *k* is the trust threshold, and *k*<*n*.
2. Joining the system: the joining process is performed by a group of at least *k* members that work together to allow access to a new node in the system.
3. Partial Certificates creation and exchange: the public and private keys of each node are created internally by each node. If a user *i* believes that a given public key k_j belongs to a given user j, then user *i* can issue a partial certificate in which k_j is bound to user *j*, signed with user *i*'s private share S_i.
4. Public Key Authentication: the public key authentication among nodes is performed via partial certificates chains. When a node *i* needs to authenticate a public key K_j of another node *j*, both nodes merge their partial trust graphs, and validate it with respect to our trust model based on the previously mentioned trust scheme. Then, node *i* tries to get a trust chain from node *i* toward node *j* in the validated partial trust graph, the authentication is completed when it is found.

So this scheme is considered a type of fully distributed public key management system that does not rely on any trusted authority. The used threshold cryptography scheme gives a resistance against malicious nodes. The problem with this type of models was the security, because dishonest users may issue false certificate to cheat other users. They overcome this problem by using private shares instead of using private keys for certificates signing.

Nen-Chung *et al.*, [21] proposed a hierarchical key management scheme. This scheme based on making key management in two-layer structure. The level 1 subgroup contains all of nodes in the subgroup. The level 2 subgroup can be decided according to the location information of nodes in the L1 subgroup. The idea in this scheme is to create a cluster head that manages information, and constructs and transmits the group key. The procedures are described as follows:

Procedure 1: L1-head selecting.

1. The weight value of each node is broadcasted to adjacent nodes. The delivery range of each node is not more than 2-hop.
2. All weight values of nodes are collected, and then the largest one is selected to be the L1-head.
3. Other nodes will register to the selected L1-head and send all information to it.

Procedure 2: L2-head selecting.

1. All nodes will send their location information to the L1-head.
2. After receiving the location information of all the nodes, according to the location information, the L1-head will classify all the nodes except the L1head into L2-subgroups.
3. The nodes of L2-subgroup will compare their weight values again and select the largest one to be the L2-head. The function of the L2-head is to manage L2-subgroup and communicate with L1-head or other L2-subgroups.

The L2-head knows the information of all the nodes in the L1-subgroup and generates the L1-subgroup key (L1GK).the L1 head transmits the L1GK to all the nodes in the subgroup. L1GK is used to encrypt all the nodes in the subgroup.

The L2-subgroups will generate their own L2-subgroup keys (L2GKs).

This scheme protects the packet security during transmission by double encryption. But its drawback is the large number of encryption and decryption operation that are needed to transmit a packet.

5.3. Decentralized Category

In this category, the multicast group is divided into sub-groups or clusters. Each subgroup is managed by a local controller which is responsible for the security management of its members in this subgroup. As an example of this approach is BALADE protocol presented in [22]. The basic idea of BALADE is to divide the multicast group dynamically into clusters. Each cluster is managed by a local controller. The local controller shares with its members a local cluster key. The multicast flow is encrypted by the source with the traffic encryption key TEK and sent in multicast to all the group members. The local controllers with the source form a multicast group GLC (Group of Local Controllers). The GLC shares a session key called KEK_{CCL}. BALADE proposed that the rekeying process of TEK is triggered by the source at each data semantic unit depending on the application. For example, a source multicasting a MP3 flow will make this operation after every song. A local controller generates and distributes to its members a local key called KEK_{CSG}. The KEK_{CSG} is renewed by the local controller, after each event of join or leave in the cluster. The local controllers are selected according to their localization. BALADE assumes that a Global Positioning System

(GPS) is available. The global controller (GC) checks periodically whether the group is highly correlated. The evaluation of the cluster cohesion is determined with a cluster cohesion parameter. The cohesion parameter is defined as the centralization index of the cluster around the LC node. With this parameter the GC decide to split the cluster and select new local controller or not. The advantage of BALADE is that the TEK is not changed for each membership event (Join or leave) but it is changed for each data unit, specific to the application.

Huihua Zhou *et al.*, proposed in [23] the two-layered MANETs model and the corresponding group key establishment scheme in detail. The main idea is to divide the nodes in the group into two parties: cell group consisting of group members and control group consisting of cell controller. A centralized key establishment is employed in cell group and a decentralized scheme is employed in control group. They proposed that nodes at each level have different communication and computation abilities. Members in cell group have equipment with communication and computation limited devices. Nodes in control group have more communication and computation power. Each node has a unique ID and one-hop neighborhood discovery mechanisms.

Group controller shares a control group key. Each group controller is responsible for transferring data within its cluster group to other cell groups. Group controllers have sufficient power and can establish point-to-point direct wireless links among each other.

Nodes inside the same cell group share a cell group key, which is used for traffic inside the same cell. The cell group key is generated and distributed by the group controller. When a new member joins a group, a key agreement between group member and group controller is established. Huihua Zhou *et al.*, replaced the long term public key certificates, when a member joins a group with implicitly Certified Public Keys method [24]. This gives the system some advantages like:

1. The space storage can be reduced.
2. The computational efforts can be reduced.
3. The communication costs can be saved.

When a group member leaves a cell group or a GC removes a compromised group member from its cell group, the GC makes group key updating and securely distributes the new group key to the remaining group members using the LKH scheme. The next section presents a hybrid key management scheme for MANETs with less number of encryption and decryption operations.

In [25] Key management integrated secure routing protocol is proposed. This protocol proposed a solution to the problem of key management (KM) and to secure routing (SR) together without separating each other as previous solutions.

6. A Hybrid Group Key Management Protocol in MANETs

In this section, a hybrid group key management protocol is presented. It's considered a mix of centralized category in subsection (5.1) and decentralized group key management as presented in subsection (5.3).

6.1. Protocol Overview

This protocol is a scalable and hybrid group key management protocol for ad hoc networks. The basic idea of this protocol is to divide the multicast group dynamically into clusters. Each cluster consists of an internal controller IC, and a number of users. There is a global controller (GC), which is responsible for the generation of the global key (GK). The

internal controllers of each cluster form with each other a group called the control group. The global controller (GC) gives the permission to a new member to form a new cluster and to be the internal controller (IC) of this cluster after checking its authenticity.

The Control Group shares a control group key. Each internal controller is responsible for transferring data from its cluster group to other cluster groups.

Nodes inside the same cluster share a cluster group key, which is used for traffic inside the same cluster. The cluster group key is generated and distributed by the internal controller.

A logical key hierarchy (LKH) tree is established in each cluster, when a new member wants to join the group, he sends a request to the GC. The GC searches with the IC's for the nearest cluster has a vacancy in its tree. Using the GPS (Global Positioning System) information, they can determine the nearest and suitable cluster. For increasing secrecy, each cluster must make an update of the cluster group key after a fixed certain period of time.

We can divide the members of the group into three types:

1. Group Controller (GC): it is the source of the multicast group. There is only one GC in the multicast group.
2. Internal Controller (IC): is a group member, forming with its local members a cluster. An internal controller generates and distributes the cluster group key to its local members. It's selected according to its localization.
3. Group member (GM): is a member of the list of nodes, authorized to join the multicast group. A group member can switch to the internal controller state according to the situation, which will be described later.

We can divide the main used keys into two types:

1. Control Group Key: it is one key shared between the control group GC and the internal controllers IC's.
2. Cluster Group Key: it is different for each cluster. It is used to encrypt all internal cluster communication.

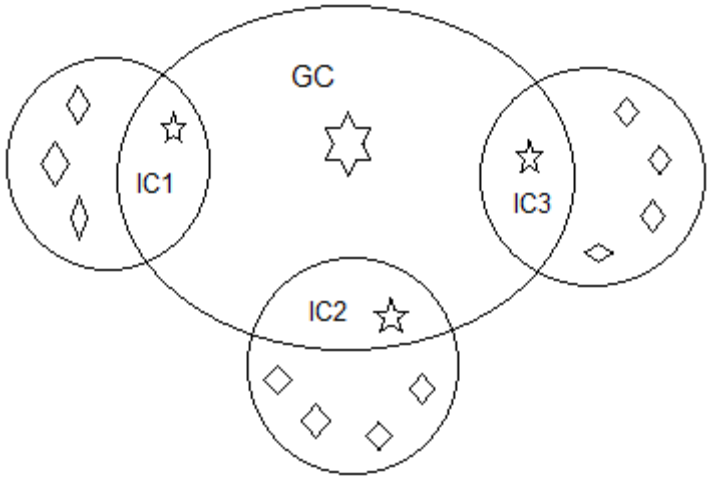

Figure 1. The Whole System is Divided into Clusters

6.2. Key Management and Distribution

The system is divided into clusters. Each cluster constructs a LKH tree with maximum fixed number of members. For simplicity, we will call the maximum fixed number of members in each cluster, MFNC. The MFNC is a variable number depends on the circumstances and the time of crowding in the corresponding cluster. After the MFNC is determined the keys construct the tree are generated by the Internal Cluster according to the MFNC. For example, as shown in Figure 2, if the MFNC=8 then the keys of the LKH are: K_{00}, K_{10}, K_{11}, K_{20}, K_{21}, K_{22}, K_{23}, $K_{24,}$ K_{30}, K_{31}, K_{32}, K_{33}, K_{34}, K_{35}, K_{36}, K_{37}. The GC determines the MFNC for each cluster. The GC takes into consideration the place and the time of each cluster, and then estimates the probable maximum number of members in this cluster according to the traffic in this cluster.

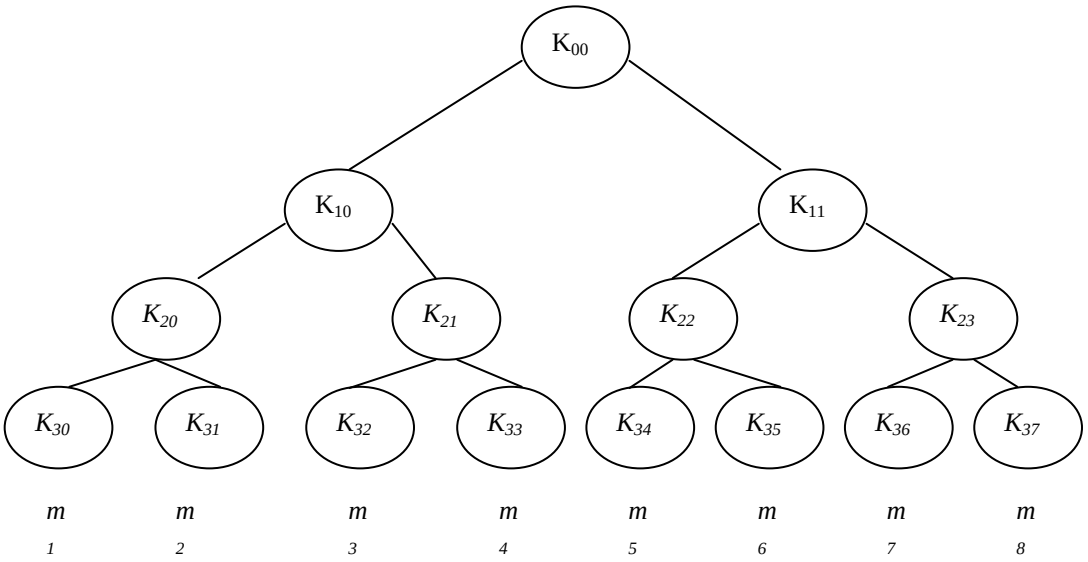

Figure 2. Each Cluster form a Logical Key Hierarchy Tree LKH

The dynamic operation for join or leave will be described in the following

Join Operation:

The new member sends a request to the GC. The GC selects the suitable cluster to this new member. The GC chooses the nearest cluster which has a vacancy. Because in LKH, each member will use a certain branch of keys, so for backward secrecy when a new member joins, the branch that will be used by this new member must be updated. Updating the branch of keys is done simply by making a simple hash function to the keys. For example, member number 5, m_5 in Figure 3 will use the predetermined keys: k_{00}, k_{11}, k_{22}, k_{34}. Note that k_{00} is the cluster group key. The new keys are computed by making a simple hash function. For example: $k'_{00} = h(k_{00})$, $k'_{11} = h(k_{11})$, $k'_{22} = h(k_{22})$, and so on.

Leave operation:

The leave operation is divided into two cases:

1. Leaving of a normal group member: when a group member leaves a cell group or a GC removes a compromised member from its cluster group, the IC of this cluster performs a

key updating and securely distributes the new group key to the remaining group members according to the LKH key establishment scheme.

2. Leaving of an internal controller: In this case the GC performs updating to the Control Group Key. The GC selects new IC according to its localization compared to the other group members. Then, the new IC makes an update to the cluster keys as in the previous case.

Moving Operation:

When an internal controller member moves within the network:, leaves the group or disappears due to any reason, it must previously, if possible, send a notification message to all its local members asking them for moving to others clusters having nearest ICs. Otherwise, if it is not possible to send a notification message, local members will, after a period of time, realize that they have lost their connectivity to their cluster, then they will attach to others' clusters.

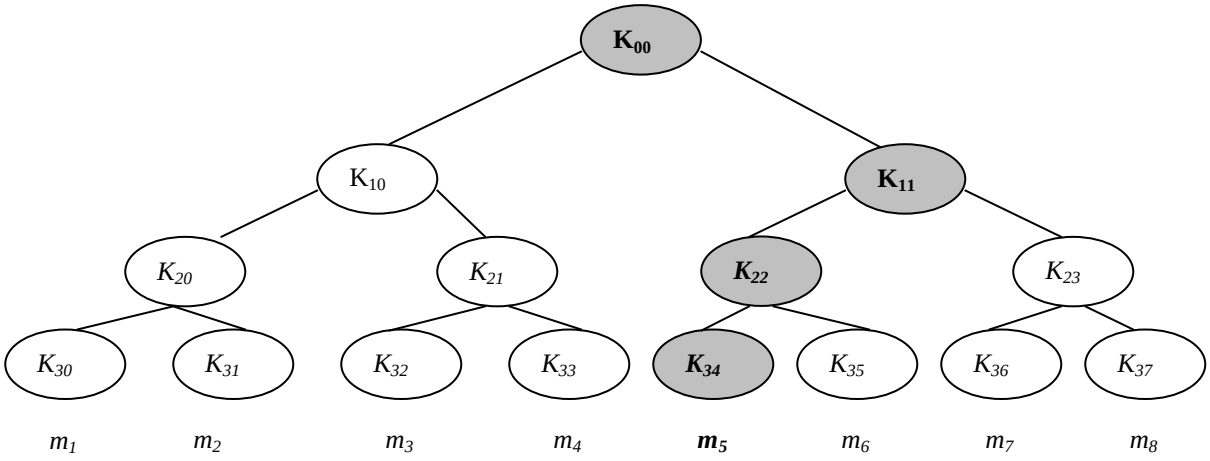

Figure 3. U_5 Joining the Group

6.3. Features of the New Protocol

1. As can we see the dynamics of one cluster group do not affect the other cluster groups. So the system doesn't suffer from the "1 affects n" phenomenon.
2. No more encryption or decryption operations are needed in case of join operation.
3. In case of a new member join, the new keys are calculated using a one-way function of the same old keys. This doesn't happen in case of leaving operation. So the system is not susceptible to collusion attack.
4. The GC makes a previous estimate of the maximum expected number of members in each cluster region.

7. Conclusions

In this paper, we have shown the characteristics and the challenges of the MANETs environment. The key management protocols dedicated to operate in wired networks are presented. Many different types of attacks that protocols in MANETs environment face are

presented. Different types of key management protocols in MANETs are also discussed. Most of the key management protocols which are suitable to operate in wired networks are not suitable to operate in MANETs environment, because of the difference in the characteristics between the two environments. A hybrid 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 one control group and number of cluster groups. Each cluster forms a LKH tree with maximum fixed members. The proposed system doesn't need any encryption or decryption operation in case of join operation. The join operation is very simple. It's only required a number of simple hash functions. In case of leave operation, each cluster is only affected. Each cluster performs cluster keys updating according to LKH key establishment scheme. So the system doesn't suffer from the "1 affects n" phenomenon.

References

[1] S. Devaraju and P. Ganapathi, "Dynamic Clustering for QOS based Secure Multicast Key Distribution in Mobile Ad Hoc Networks", IJCSI, vol. 7, no. 5, **(2010)** September, pp. 30-37.
[2] K. Drira, H. Seba and H. K Heddouci, "ECGK: An efficient clustering scheme for group key management in MANETs", Computer Communications, **(2010)**, pp. 1094-1107.
[3] C. Kei Wong, M. Gouda and S. S. Lam, "Secure Group Communications using Key Graphs", Proceedings of ACM SIGCOMM, Vancouver, British Columbia, Canada, **(1998)** August 31-September 4, pp. 68-79.
[4] D. Wallner, E. Harder and R. Agree, "Key Management for Multicast: Issues and Architectures", RFC2627, **(1999)**.
[5] S. Mittra, "Iolus: A framework for scalable secure multicasting", SIGCOMM, **(1997)**, pp. 277-288.
[6] L. R. Dodeti, S. Mkherjee and A. Samal, "Scalable secure one-to-many group communication using dual encryption", Computer Communications, vol. 23, no. 17, **(2000)**, pp. 1681-1701.
[7] L. R. Dondeti, S. Mukherjee and A. Samal, "Scalable secure one-to-many group communication using dual encryption", Computer communications, vol. 23, no. 17, pp. 1681-1701, **(2000)**.
[8] T. Hardjono and L. Dondeti, "Multicast and Group Security", computer Security Series, Artech House, **(2003)**.
[9] M. Ilyas, "The handbook of Ad Hoc Wireless Networks", CRC Press, **(2003)**.
[10] X. Zhang, "Malicious packet dropping: how it might impact the TCP performance and how we can detect it", Network Protocols, Proceedings, IEEE International Conference, **(2000)** November 14-17.
[11] W. Wang, "Defending against Collaborative Packet Drop Attacks on MANETs", Joint Workshop on Dependable Network Computing and Mobile Systems (DNCMS) and Field Failure Data Analysis (F2DA) **(2009)** September 27.
[12] S. Gavaskar, R. Surendiran and Dr. E. Ramaraj, "Three Counter Defense Mechanism for TCP SYN Flooding Attacks", International Journal of Computer Applications, vol. 6, no. 6, **(2010)** September, pp. 12-15.
[13] N. Weaver, V. Paxson, S. Staniford and R. Cunningham, "A Taxonomy of Computer Worms", First Workshop on Rapid Malcode (WORM), **(2003)**.
[14] T. Kaya, G. Lin, G. Noubir and A. Yilmaz, "Secure multicast groups on Ad Hoc networks", Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, **(2003)**, pp. 94-102.
[15] A. Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA broadcast authentication protocol", RSA Laboratories Cryptobytes, vol. 5, no. 2, **(2002)**, pp. 2-13.
[16] S. Zhu, S. Setia, S. Xu and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad Hoc Networks", Technical report, **(2004)** February.
[17] L. Lazos and R. Poovendram, "Energy-aware secure multicast communication in Ad Hoc networks using geographical location information", IEEE International Conference on Acoustics Speech and Signal Processing, **(2003)**, pp. 201-204.
[18] C. Wong, M. Gouda and S. Lam, "Secure group communications using key graphs", ACM SIGCOMM, **(1998)**, pp. 68-79.
[19] J. Kong, Y.-Z. Lee and M. Gerla, "Distributed Multicast Group Security Architecture for Mobile Ad-hoc Networks", IEEE Wireless Communications & Networking Conference (WCNC), Las Vegas, Nevada, USA, **(2006)** April.
[20] M. Omar, Y. Challal and A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks", computer&Security, **(2009)**, pp. 199-214.
[21] N.-C. Wang and S.-Z. Fanf, "A hierarchical Key Management Scheme for Secure Group Communications in Mobile Ad Hoc Networks', Journal of systems and software, **(2007)**, pp. 1667-1677.

[22] M.-S. Bouassida, I. Chrisment and O. Festor, "Group Key Management in MANETs", Campus Scientifique B.P.239, **(2006)** May 11.
[23] H. Zhou, M. Zheng and T. Wang, "A Novel Group Key Scheme for MANETs", Advanced in control Engineering and Information Science, Procedia Engineering, **(2011)**, pp. 3388-3395.
[24] Y. Zheng, "Shortened Digital Signatures", Signcryption and Compact and Unforgeable Key Agreement Schemes. Submission to IEEE P1363a: Standard Specifications for Public-Key Cryptography, **(1998)**.
[25] S. Zhao, R. Kent and A. Aggarwal, "A key management and secure routing integrated framework for Mobile Ad-hoc Networks", Ad Hoc Networks, vol. 11, **(2013)**, pp. 1046-1061.

