



## Cluster Based Multiple Group Key Management for Mobile Multicast

**Asha Raj**

M.Tech Student, KMEA,  
CSE Department, MG University  
Kerala, India

**Abeera V P**

Assistant Professor, KMEA,  
CSE Department, MG University  
Kerala, India

---

**Abstract**— Due to the emergence of mobile devices and group based services, key management has become the major booming topic in mobile multicast communication. Within a single network, multiple multicast services could co-exist and mobile users can subscribe to these services. Existing group key management (GKM) schemes are not capable of handling multiple multicast services. They are intended for single group service. Also they are not efficient in handling keys, and results in huge rekeying overheads in case of multiple multicast environments. A novel GKM scheme, called cluster based multiple group key management (CMGKM) scheme, is proposed in this paper. This framework efficiently handles keys in multiple multicast environments and reduces the rekeying overheads. It also eliminates one-affect-n phenomenon and single point of failure, and provides high security.

**Keywords**— Group key management, mobile multicast, wireless networks, rekeying, security, encryption

---

### I. INTRODUCTION

The development of wireless networks and the emergence of portable devices such as smart phones, tablets, etc have increased to meet the demand for multicast applications. Multicast is an efficient technique for delivering group oriented applications such as video conferencing, interactive group games, mobile TV services, over the internet. It utilizes one-to-many and many-to-many communication mechanism. Mobile Ad-hoc networks consist of a collection of mobile hosts with wireless network interfaces forming a temporary network. They are special type of wireless networks without any fixed administration or centralized administration.

Due to open access in wireless networks, multicast services over the air have become vulnerable to various security attacks such as denial of service attack, impersonation attack, etc. In-order to deliver multicast content securely, an access control mechanism ensuring authentication, integrity and confidentiality is necessary. Cryptography is an important and powerful tool for secure services that converts plaintext into cipher-text. There are basically 2 main approaches – symmetric-key/secret-key approach and asymmetric-key/public-key approach. In symmetric-key approach, the same key is used for both encryption and decryption. While in asymmetric-key approach, different keys are used for encryption and decryption.

A standard approach to provide access control mechanism [1] for safe multicast communication is by using a symmetric group key. Group messages encrypted with the secret key can be decrypted by valid group members holding similar key assuring secure group communication. Confidentiality and integrity are maintained which ensures that non group members cannot read the data and also the data cannot be modified or deleted in any unauthorized way.

The most important part of any secure communication is key management. It deals with generation of keys, distribution of keys to the members and key maintenance. In mobile multicast environment, members frequently join and leave a group. Due to this group membership dynamics, maintaining an efficient key management system is a challenge. This triggers update of the key through rekeying process. The following are the missions carried out by group key management:

- Key Generation: It refers to the generation of group key and all supporting keys.
- Key Distribution: It refers to the efficient, secure and reliable delivery of keying materials to the group members.
- Key updating/Rekeying: It refers to the process of changing the group key and supporting keys.

The following are the major security requirements for group key management in mobile wireless network:

- Group key secrecy: It ensures that non group members cannot obtain any group key.
- Backward secrecy: It restricts access to any prior messages after a member joins.
- Forward secrecy: It restricts access to any future messages after a member leaves.

Performance requirements include:

- Low communication, computation and storage overhead.
- Scalability for large dynamic groups.
- Reliable distribution of key update messages.

Due to the emergence of computationally fast mobile devices and various group based applications, it is predictable that in the future, multiple multicast groups will co-exist within the same network. Such a situation will cause ample key management overhead at the service provider for supporting multi-group services. The existing Group Key Management (GKM) schemes for secure wired and wireless networks will suffer from rekeying performance, as they are targeted for a single multicast service. Fig 1 illustrates an example of a multiple multicast service environment. Members under same service group subscribe to same set of services. For example, users U1 and U2 under service group SG1 subscribe to cinema and sports services. According to existing GKM schemes, each multicast service is independently controlled by a single GKM protocol.

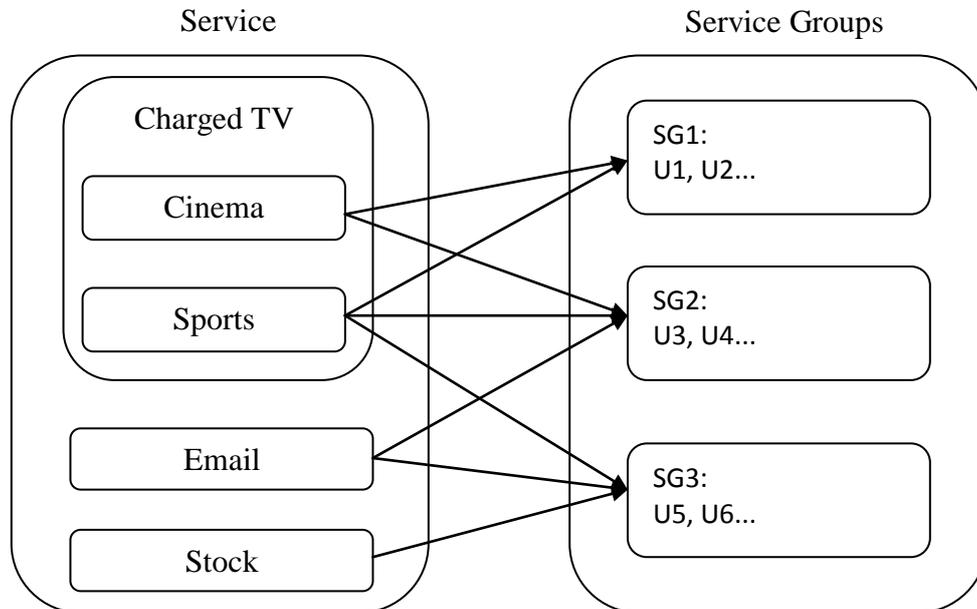


Fig 1: An example of multiple multicast services and groups

When a member dynamically leaves or joins subscribed services, all the affected services would require independent rekeying procedure hence causing considerable amount of rekeying overhead. In case of mobile environment, a handover member is considered as departing from the current cluster followed by a join at the target cluster. Thus rekeying overhead is induced twice due to host mobility. In order to prevent service latency and also to reduce rekeying overhead, a trivial access control mechanism with efficient group key management need to be addressed.

A novel GKM protocol for multiple multicast service groups, called cluster based multiple group key management (CMGKM) scheme is proposed here. It reduces rekeying, communication and storage overheads and also eliminates single point of failures and one-affect-n phenomenon. In CMGKM, the key management tasks are delegated to the intermediate cluster managers. The rest of the paper is organized as follows: Related work is described in Section II. In Section III, the proposed CMGKM scheme is described in detail, and compared with other existing schemes. Finally, Section IV concludes the paper.

## II. RELATED WORK

Existing Group key management (GKM) protocols for wired networks [2] can be classified into 3 main classes:

- Centralized key management protocols
- Decentralized key management protocols
- Distributed key management protocols

Centralized key management protocols depend on a central server for key generation and distribution, and hence it suffers from single point of failure. It is also not capable of supporting multiple memberships. The key management for centralized scheme establishes separate keys for each multicast session. Because of this, a user participating in multiple sessions needs to handle huge number of keys. Decentralized key management protocols divide the network into different sub networks. Each sub network is handled by a subgroup manager who is responsible for key generation and distribution. Hence it eliminates single point of failure and distributes load evenly. Distributed key management protocols have no explicit domain key distributors. All the members participate in group key generation, and hence it is also known as contributory scheme.

Work in [3] divides group key management protocols into 2:

- Network Independent based
- Network dependent based

Centralized, decentralized and distributed are categorized under network independent based schemes. Network dependent based schemes are further classified as Tree based and Cluster based schemes. Tree based scheme maintains a

tree like structure where the intermediate nodes represents the keys and the leaf nodes represents group members. Group key is stored in the root of the tree. When a new member joins, a leaf node is added and all keys from the new leaf node's parent in the path to the root are compromised and are changed. Cluster based schemes divides the main network into sub-networks. All members in the cluster share the same key.

Group key management protocols can be further categorized into 2 [5]:

- Common Traffic Encryption Key (TEK) approach
- Independent TEK per sub group.

Centralized and distributed key management protocols use common TEK, whereas decentralized key management protocols use independent TEK per subgroup. Common TEK approach exploits one TEK for all members which can result in one-affect-n phenomenon. Independent TEK per sub group exploits independent TEK for each subgroup. Thus rekeying is localized which eliminates one-affect-n phenomenon. These GKM protocols cannot be extended for wireless mobile networks as they did not consider host mobility.

Few GKM protocols have been proposed for wireless mobile networks [6] which consider rekeying issues, dynamic membership change and dynamic location change. These protocols are not capable to handle multiple group services. Some of the basic inter-area rekeying algorithms are:

- Baseline Rekeying
- Immediate Rekeying
- Delayed Rekeying
- Periodic Rekeying

Baseline rekeying is a direct approach for handling mobility. It treats movement as a leave from old cluster followed by a join to a new cluster. It halts the data transmission during rekeying process. Thus it can lead to long service disruptions. Immediate rekeying updates the key without disrupting the data transmission. Delayed rekeying postpones the rekeying process until a particular criterion is satisfied. This causes members to accumulate multiple keys so that it can be reused when the cluster is visited again. This reduces rekeying overhead by increases storage overhead. Periodic rekeying updates the keys at particular time intervals. Major drawback is that the departing members are not removed immediately and the new members are delayed till the beginning of the next time interval. Most of the GKM protocols adopt delayed rekeying strategy which also suffers from one-affect-n phenomenon.

Based on the techniques used to distribute the TEK's, the group key management protocols are further classified as [4]:

- Pair-wise Keys
- Key Hierarchy
- Membership Driven
- Time-Driven Rekeying
- Ring-based cooperation

Pair-wise keys make use of a secret key with each group member to establish secure channel with the server. Key hierarchy is similar to tree based schemes which maintains a tree of keys. Membership driven approach performs rekeying whenever a join or a leave operation is performed within the group. Time-driven approach performs rekeying at specific period of time. IT is similar to periodic rekeying. Ring based cooperation forms a virtual ring of the group members. Each member  $M_i$  contributes for the group key generation and communicates with member  $M_{i+1}$ . Group key is generated after  $(n-1)$  rounds. This approach is not suitable for dynamic groups. To overcome these challenges, a cluster based group key management protocol for multiple multicast services is proposed here.

### **III. PROPOSED SYSTEM**

#### **A. CMGKM Framework**

The Cluster based multiple group key management (CMGKM) adopts a two-tier decentralized framework as shown in Fig 2:

- First level is the domain level which is controlled by Domain Key Distributor (DKD).
- Second level is the cluster level which is controlled by Cluster Key Distributor (CKD).

Each cluster consists of set of users subscribed to different services and maintains independent TEK per cluster. Here the rekeying process is localized and thus it eliminates one-affect-n phenomenon. When a user joins or leaves a cluster, the rekeying is handled without affecting the entire system. One of the main differences between a centralized scheme and decentralized scheme is that, in the former, the DKD is responsible for key management, whereas in the later, the Cluster/Area key Distributor is responsible for key management. Each CKD communicate with each other to handle the handoff procedure. It also provides scalability, security and high performance.

This framework satisfies the following key management security requirements:

- Forward secrecy: It ensures that the user is restricted from accessing the future messages or services after he leaves.
- Backward secrecy: It ensures that the user is restricted from accessing the prior messages after he joins. Pair-wise Keys

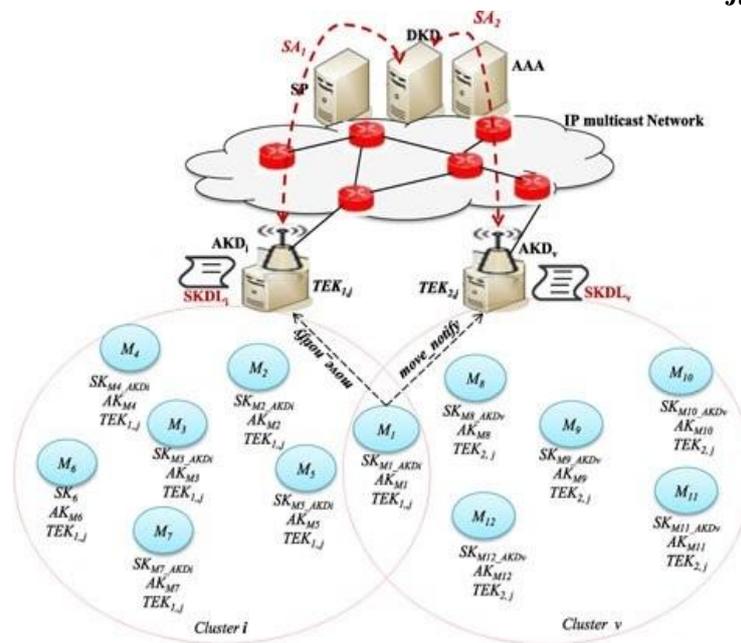


Fig 2: CMGKM Framework

### B. Key Generation Algorithm

The initial key generation is done at the domain level by the DKD at the time of group setup. The rest of the procedure is handled at the cluster level by the CKD. The services within each cluster are defined; each service has a service key (SK) and each cluster has a cluster key (CK). The first phase is the registration phase for a member which can be performed by the member itself or by the administrator. A registered member holds a valid user key (UKMi) for authentication. The following are the steps for key generation:

1. Group key (GK) is generated by appending the SK's of all the subscribed services.
2. GK is encrypted using CK (AES algorithm).
3. UKMi is appended to the encrypted GK.
4. Final key is generated by appending the cluster id to the key generated in step 3.

When a user is subscribed to multiple services, all the service keys are appended together to form the group key. For providing security, the group key is encrypted using CK. User authentication is done by appending UKMi to the encrypted group key. For handling mobility, the cluster details are appended to the key and the final key is generated. These keys are shared between CKD's during a member handoff.

### C. Rekeying Algorithm

When a member joins, it is handled in two ways:

- As a new entry
- As a leave from old cluster and join in the new cluster (Member handoff)

New entry of a member is handled as described in the previous section. When a member is moved from one cluster i to another cluster j, the session key is passed to the new CKDj. The key is decrypted to retrieve the details of the subscribed services and a new temporary key is generated to access those services in the new cluster. This framework provides the flexibility to the user to join or leave any subscribed services at any time. The user is restricted to view the subscribed services only if it is available in the current cluster.

Leaving of a member from a group/cluster can happen due to 2 reasons:

- Expiry of the subscribed services.
- Mobility – leaving from cluster i and joining to cluster j.

When any of the subscribed services expire, the service is removed from the user and a new key is generated through rekeying process. When a user is moved from his home cluster to a temporary cluster, his home cluster key to access the services is not deactivated. Instead a new key is generated in the target cluster for temporarily accessing the services. This eliminates the need for rekeying in case of users who frequently move between clusters.

The following are the steps for updating the key (rekeying):

1. The cluster id is retrieved from the key.
2. Using the CK, the key is decrypted.
3. Services subscribed by the user are retrieved.
4. A temporary key is generated as described in key generation algorithm in section B. Here, both the cluster identifiers will be appended.

#### D. CMGKM comparison with Existing Key Management Protocols

This section does comparison study of CMGKM with some of the existing key management protocols. CKD-CKD communication link is introduced in CMGKM for minimized rekeying performance and fast handoffs. CMGKM eliminates 1-affect-n phenomenon, supports multiple group services, eliminates single point of failure and does authentication at movement. Table 1 shows the comparison of CMGKM with BS, IR and FEDRP

TABLE I COMPARISON STUDY

CMGKM Comparison with Existing Key Management Protocols				
Evaluation Criteria	BS	IR	FEDRP	CMGKM
Decentralized framework	Y	Y	Y	Y
Number of layers	2	2	2	2
Forward secrecy on member move	Y	Y	N	Y
Backward secrecy on member move	Y	Y	Y	Y
1-affect-n phenomenon	Y	Y	Y	N
Localize rekeying at member move	N	Y	Y	Y
CKD to CKD communication link	N	N	N	Y
Support multiple group services	N	N	N	Y
Single point of failure	Y	Y	Y	N
Authentication at move	N	N	N	Y

#### IV. CONCLUSIONS

To improve the key management in multiple multicast group environment networks, a new cluster based multiple group key management (CMGKM) scheme has been proposed in this paper. It ensures both forward and backward secrecy while maintaining diverse subscriptions. It improves key management performance when members perform multiple moves between clusters and also handles multi group services efficiently. As traditional schemes are targeted for single service, CMGKM adopts a new key generation and rekeying strategy for multiple services. It also performs authentication during member handoffs. It adopts a two-tier decentralized framework with independent TEK per cluster. The first level is the domain level controlled by DKD which handles the initial key generation. The rest of the processes are handled at the cluster level by the CKD. This localizes the rekeying process, eliminates one-affect-n phenomenon, reduces load at the core network, prevents bottlenecks and also gives scalability to DKD. In future, it is predictable that due to the emergence of wireless networks and the development of portable devices, multiple multicast applications will exist within same network. CMGKM is expected to provide a feasible solution for secure and efficient management of multiple services.

#### ACKNOWLEDGMENT

The authors would like to sincerely thank the editors and anonymous reviewers for their valuable comments.

#### REFERENCES

- [1] T. T. Mapoka, S. J. Shepherd and R. A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast," IEEE Transactions on Mobile Computing, vol. 14, No.8, August 2015.
- [2] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," ACM Computer Surveys, vol. 35, pp. 309–329, Sept. 2003.
- [3] T. T. Mapoka, "Group key management protocols for secure mobile multicast communication: A comprehensive survey," Int. J. Comput. Appl., vol. 84, pp. 28–38, Dec. 2013.
- [4] Y. Challal and H. Seba, "Group key management protocols: A novel taxonomy," Int. J. Inf. Technol., vol. 2, pp. 105–119, 2005.
- [5] T. Hardjono, B. Cain, and I. Monga, "Intra-domain group key management for multicast security," IETF Internet draft, Sept. 2000.
- [6] B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, and C. Zhang, "Secure group communications for wireless networks," in Proc. Commun. Netw.- Centric Oper.: Creating Inf. Force. IEEE Military Commun. Conf.,2001, vol. 1, pp. 113–117.