



# Novel Multicast Key Management Scheme for PMIPv6-Based LTE Networks

**Ming-Chin Chuang**

Institute of Information Science, Academia Sinica, Taiwan, R.O.C.

**Email address:**

[speedboy@gmail.com](mailto:speedboy@gmail.com)

**To cite this article:**

Ming-Chin Chuang. Novel Multicast Key Management Scheme for PMIPv6-Based LTE Networks. *American Journal of Electrical and Computer Engineering*. Vol. 1, No. 2, 2017, pp. 50-60. doi: 10.11648/j.ajece.20170102.11

**Received:** March 27, 2017; **Accepted:** April 17, 2017; **Published:** June 2, 2017

---

**Abstract:** Multicast services grow up quickly and thus they urgently call for a secure mechanism to provide the confidentiality and privacy of communications. Recently, multicast issues in Proxy Mobile IPv6 (PMIPv6) networks have generated a great deal of interest among researchers, and several multicast schemes had been proposed. However, these schemes do not take security issues into account. In an attempt to fill that research gap, we propose a dual multicast key management scheme for secure group communications in PMIPv6-based Long Term Evolution (LTE) networks. This scheme satisfies the requirements for forward and backward secrecy. Moreover, the performance analysis demonstrates that the proposed scheme incurs low communication and storage costs. Finally, we provide guidelines for Internet service providers (ISPs) to select the suitable multicast key management architecture.

**Keywords:** Multicast, Confidentiality, Privacy, Proxy Mobile IPv6, Key Management

---

## 1. Introduction

With the rapid development of wireless technologies, mobile devices, such as cellular phones, smart phones, notebooks, and personal digital assistants (PDAs), are becoming increasingly popular. The major advantage of such devices is that they enable users to access all kinds of services anytime, anywhere.

For continuous services, the IETF NETLMM working group proposed a network-based mobility management scheme called Proxy Mobile IPv6 (PMIPv6) [1] to reduce the handover latency of host-based mobility management schemes [2]-[4]. PMIPv6 also supports mobile nodes (MNs) with IP mobility without requiring the participation of MNs in any mobility-related signaling. In addition, the MN does not need to change its IP address when it moves around the same localized mobility domain (LMD). Such a solution is being standardized within the 3GPP System Architecture Evolution/Long Term Evolution (SAE/LTE) Standard [19] for next-generation networks. Figure 1 depicts the LMA-based and MAG-based multicast methods in PMIPv6-based LTE networks. The serving gateway (S-GW) includes the mobile access gateway (MAG) functionality which is responsible for detecting the movements of an MN and performs mobility-related

signaling with the local mobility anchor (LMA) in place of the MN. The PDN gateway (P-GW) provides the access in different packet data networks (PDN) and includes the LMA functionality which maintains the binding cache entries for currently registered MNs. The authentication, authorization, and accounting (AAA) server is responsible for authenticating the MN. The 3GPP LTE specification introduces the access network discovery and selection function (ANDSF) [20] to search for the suitable neighbor access networks. The mobility management entity (MME) is in charge of all the control plane functions related to subscriber and session management, the home subscriber server (HSS) is the concatenation of the home location register (HLR), and the evolved node B (eNB) as a base station needs to manage the radio resource.

In recent years, multicast applications, such as video on demand (VoD), IPTV, video conferencing, and e-learning, have become increasingly popular. These applications can be implemented more easily in wireless networks than in wired networks because a single transmission can be received by all nodes within the transmission range due to the broadcast medium. Based on Multicast Listener Discovery (MLD) [9] or the Internet Group Management

Protocol (IGMP) [10] in MIPv6 networks, two mobile multicast methods, Bi-directional Tunnel (BT) and Remote Subscription (RS), were proposed in [5]-[8]. Recently, a number of modified BT and RS methods that are compatible with PMIPv6 networks have been developed. For example, [11]-[14] [23] proposed MAG-based and LMA-based multicast mechanisms for PMIPv6 networks, as shown in figure 1. Consequently, the key distribution center (KDC) is responsible for generating, distributing, and updating the multicast key. The service provider (SP) obtains the multicast key from the KDC and can deliver the encrypted multimedia content to MNs via MAG-based or LMA-based multicast methods.

The objectives of MAG-based and LMA-based multicast mechanisms are to reduce handoff latency and end-to-end transmission delay and thereby improve the quality-of-service (QoS). The MAG-based method is similar to the RS method in that the MN joins the multicast group directly and receives multicast content through the current MAG without passing through the LMA. Therefore, the MAG-based method has lower end-to-end transmission delay. The LMA-based method is similar to the BT method in that the MN joins the multicast group through the LMA and receives the multicast content via the MAG-LMA tunnel. The MN does not rejoin the group as it moves around the same LMD because it joins the multicast group through the LMA. Besides, the LMA-based method has lower join and handoff delay. As a result, the LMA-based method is fit for high speed environment and the MAG-based method is fit for stable environment.

Unfortunately, these multicast mechanisms do not take the security issue into account, even though many group communication services require a secure mechanism to protect the privacy of valid users. In wireless multicasting, cryptography is normally employed to ensure that communications are secure. Specifically, a group key shared by all members of the multicast group is used to encrypt and decrypt the communication content. As a result, key management is a major research issue in the secure wireless multicast. To address the issue, we propose an MAG-based multicast key management scheme (M-MKMS) and a LMA-based multicast key management scheme (L-MKMS) for secure group communications in PMIPv6-based LTE networks to satisfy the requirement for forward and backward secrecy.

The remainder of the paper is organized as follows. In Section 2, we discuss the preliminaries, and in Section 3 we describe the proposed scheme in detail. Section 4 displays the performance analysis of M-MKMS and L-MKMS, and then we provide some guidelines for ISPs to select the suitable multicast key management architecture. Section 5 contains some concluding remarks.

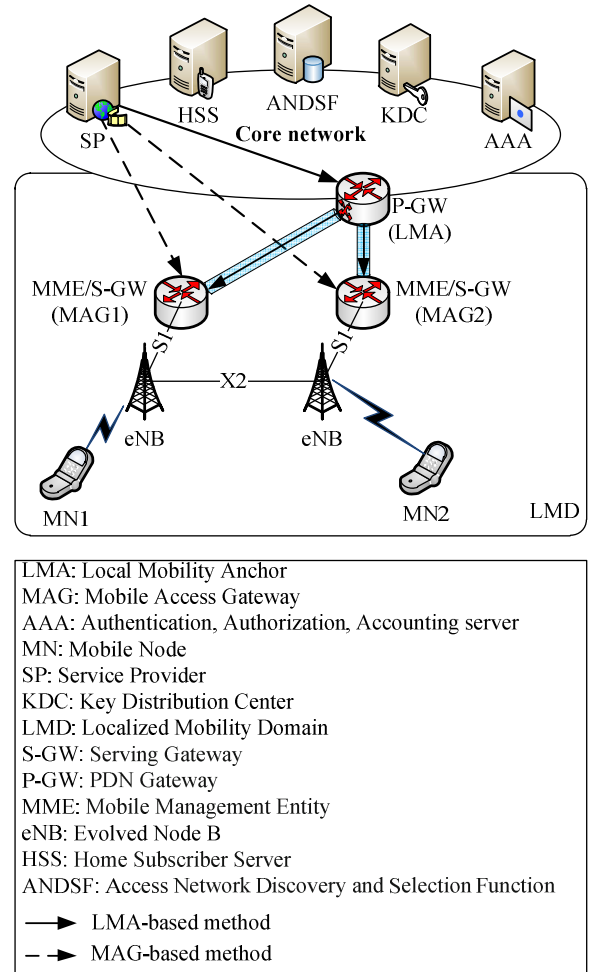


Figure 1. LMA-based and MAG-based multicast methods in PMIPv6-based LTE networks.

## 2. Preliminaries

### 2.1. Security Requirements

The multicast key must be renewed when a mobile node joins, departs, and hands off a multicast group. The multicast key management scheme must satisfy the forward and backward secrecy requirement.

- Forward secrecy: The multicast key must be changed to ensure that a departing member cannot decrypt data transmissions after he/she has left the multicast group.
- Backward secrecy: The multicast key must be changed to ensure that a new member cannot decrypt data transmitted before he/she joined the multicast group.

### 2.2. Logical Key Hierarchy (LKH)

The Logical Key Hierarchy (LKH) [15] [16] [22] protocol is one of the most widely used group key management schemes. Figure 2 shows a typical LKH key management tree architecture which is composed of key nodes (i.e.,  $K_1$ - $K_4$ ,  $K_{12}$ ,  $K_{34}$ , and  $K_{14}$ ) and member nodes (i.e.,  $M_1$ - $M_4$ ). The key node means a key in the key tree and the member node means an MN in the multicast group. Moreover, the key

nodes are divided into three kinds: a group key ( $GK$ ), key encryption keys ( $KEKs$ ), and individual keys ( $IKs$ ). In the key tree of the figure 2, the root node is the  $GK$  to guarantee secure communications among the group members; the internal nodes are  $KEKs$  to encrypt the updated messages sent to valid MNs; and the leaf nodes are  $IKs$ . Each group member (e.g.,  $M_i$ ) needs to store an  $IK$  associated with its leaf node (e.g.,  $K_i$ ) and the  $KEKs$  corresponding to each ancestor node (e.g.,  $K_{12}$ ) on the key path from its parent node to the root node (e.g.,  $K_{14}$ ). All group members share a universal group key held by the tree's root node (i.e.,  $K_{14}$ ). In the group, the sender uses the  $GK$  to encrypt the data for transmission and then the recipient uses the  $GK$  to decrypt the encrypted data. The KDC also manages the rekey procedure when a multicast member (e.g.,  $M_4$ ) joins/departs the group. To ensure backward/forward secrecy, the KDC must change all the keys on the key path from the leaf node of the joining/departing member to the root node (e.g.,  $K_4$ ,  $K_{34}$ , and  $K_{14}$ ). Finally, the KDC notifies a new  $GK$  to all group members.

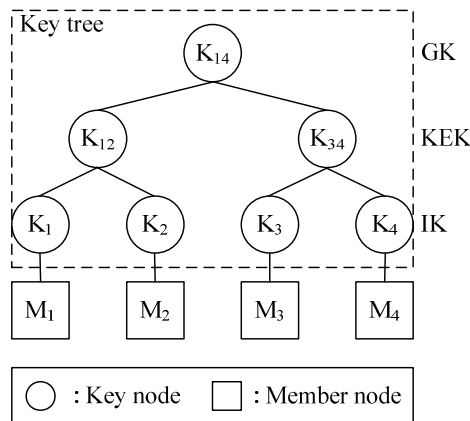


Figure 2. The LKH key management tree architecture.

Although the LKH scheme satisfies the forward and backward secrecy, reduces the number of rekey messages, and encryption operations, it suffers from the “one affects all” problem [17], where one member (i.e., a joining or departing member) affects all the other group members. In addition, the LKH scheme cannot rekey messages efficiently because its key tree structure is independent of the network topology [18]. References [24] and [25] proposed new key management schemes, but their schemes cannot be applied in PMIPv6-based multicast environment directly.

### 3. Multicast Key Management Scheme (MKMS)

In this section, we describe the proposed multicast key management scheme (MKMS) architecture, which is comprised of the MAG-based MKMS (M-MKMS) and the LMA-based MKMS (L-MKMS) schemes. In LKH, the KDC manages all members (i.e., it stores lots of keys). Moreover, the KDC performs the rekey procedure frequently resulting

in high communication cost when a multicast member often joins/departs the group. Therefore, we modify the LKH scheme to mitigate the “one affects all” problem by a two-level key management architecture. Thus, the KDC does not need to manage the keys of all members which results in lower storage cost, and performs the rekey procedure locally to reduce the communication cost. Moreover, our proposed M-MKMS and L-MKMS are based on a decentralized approach where the MAGs or the LMAs help manage the user keys locally and thus share the load of the KDC. These schemes also match the key management tree to the network topology, which can reduce the unnecessary rekey behavior [17] [18]. Finally, in this architecture, the KDC is not responsible for revoking and updating all the keys of the members. It only needs to manage the group key that it issues to the MAGs/LMAs. Before describing the proposed scheme in detail, we explain the notations used in the remainder of the paper, as shown in Table 1.

Table 1. Notations.

Symbol	Description
{mag}	A mobile access gateway
{MAG}	A set of mobile access gateways
{lma}	A local mobility anchor
{LMA}	A set of local mobility anchors
{mn}	A mobile node
{MN}	A set of mobile nodes
$A \rightarrow B$	User A sends a message to user B via unicast
$A \rightarrow B$	User A sends a message to user B via multicast or broadcast
GK	Group key
Local-GK	Localized group key
Domain-GK	Domain group key
KEK	Key encryption key
IK	Individual key
PK	Personal key

#### 3.1. M-MKMS

In the MAG-based multicast method, the MN joins the multicast group directly and receives the multicast content through the current MAG. As a result, the MN needs to rejoin the multicast group again when it attaches to a different MAG, and thus the M-MKMS method needs not include a handoff operation. The key management procedure under M-MKMS is divided into two independent levels. The LKH scheme is employed among KDC and MAGs (i.e., Level-1), and our proposed M-MKMS is used as a local group key management procedure applied in the serving range of each MAG (i.e., Level-2). Thus, the KDC does not need to manage the keys of all members resulting in lower storage cost and performs the rekey procedure locally to reduce the communication cost. We assume that the MAG is capable of supporting the key management procedure. Thus, the MAG plays two roles: (i) a member node, and (ii) a key node. Figure 3 shows the key management architecture under M-MKMS.

##### 3.1.1. Multicast Data Transmission

In figure 1, the SP encrypts the multicast data with the  $GK$  and sends it to the MAG, which then decrypts the data with

its *GK*. Next, the MAG encrypts the data with the *Local-GK*, and multicasts it to the members who use the *Local-GK* to obtain the data. Note that the role of *Local-GK* is similar to *GK*, but it belongs to the localized *GK* in the serving range of the MAG. In addition, the relation between *GK* and *Local-GK* is independent (i.e., *Local-GK* does not affect *GK*; *GK* does not change when *Local-GK* changes).

### 3.1.2. Join Operation

When an MN joins a group, backward secrecy must be ensured so that the new member cannot decrypt any previously transmitted multicast data. There are two possible scenarios when an MN wants to join a multicast group: (i) the MAG is not a member of the group; or (ii) the MAG is already a member of the group. Note that the MAG generates the *Local-GK* for the MN independently. Hence, the MAG does not change the *GK* when the MN attaches to a different MAG. The steps of the join operation are as follows.

Step 1:  $\{mn\} \rightarrow \{mag\}$ : When an MN wants to join a multicast group, it sends a group join message to the current MAG.

Step 2: On receipt of message, the MAG checks whether it is a multicast member of the group that the MN wants to join. If it is not a member, it executes the LKH scheme (i.e., it satisfies the backward secrecy) to join the multicast group and obtain the new *GK*. Then, the KDC notifies the new *GK* to all MAGs. Otherwise, the MAG performs Step 3.

Step 3:  $\{mag\} \rightarrow \{mn\}$ : After accepting the MN's join request, the MAG generates a new *Local-GK* to guarantee backward secrecy and shares the pair-wise personal key (*PK*) with the new member. Note that *PK* is only known to the MAG and the MN. The MAG encrypts the new *Local-GK* with the *PK* and sends it to the new member. In this step, the new member cannot decrypt the previous data because he/she does not know the old *Local-GK*.

Step 4:  $\{mag\} \rightarrow \{MN\}$ : The MAG encrypts the new *Local-GK* with the old *Local-GK* and then broadcasts the encrypted new *Local-GK* to other multicast members.

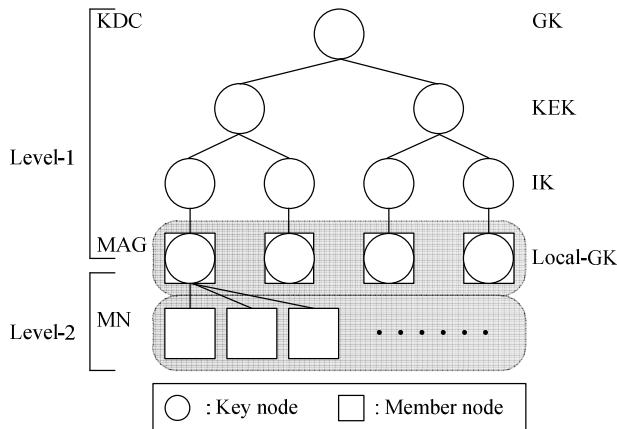


Figure 3. Key management in M-MKMS.

### 3.1.3. Leave Operation

When a member leaves the group, forward secrecy must be guaranteed so that the member cannot decrypt subsequent

data transmissions. There are also two possible scenarios when an MN wants to leave a multicast group: (i) there are no other multicast members in the MAG; or (ii) some multicast members are still located in the MAG. A leave operation can be initiated by the MN. The steps of the procedure are as follows.

Step 1:  $\{mn\} \rightarrow \{mag\}$ : When an MN wants to leave the multicast group, it sends a group leave message to the current MAG.

Step 2: On receipt of the message, the MAG checks whether there are other members in the multicast group. If the MN is the last member of the multicast group, the MAG executes the LKH scheme (i.e., it satisfies the forward secrecy) to depart the group. Then, the KDC broadcasts the new *GK* to all remaining MAGs. Otherwise, the MAG performs Step 3.

Step 3:  $\{mag\} \rightarrow \{MN\}$ : The MAG generates a new *Local-GK*, encrypts this new *Local-GK* with each member's *PK*, and sends it to each member where locates in the same serving range of the MAG. The *Local-GK* received by each member is encrypted with his/her *PK*. The leaving MN cannot decrypt the later data since it does not receive the new encrypted *Local-GK* sent from the MAG. Therefore, this scheme guarantees the forward secrecy.

### 3.2. L-MKMS

The proposed L-MKMS scheme adopts a two-level key management architecture, as shown in figure 4 to match the key management tree to the mobile network's topology. We assume that the LMA is also capable of supporting the key management procedure. The entire wireless network is divided into several localized mobility domains (LMDs), and the LMA manages the MAGs within its domain. Under the LMA-based multicast method, the MN does not rejoin the group when it moves around the same LMD because it joins the multicast group through the LMA. Therefore, we implement a "Handoff Operation" in L-MKMS when the MN moves around different MAGs in the same LMD. The handoff operation is the main difference between the L-MKMS scheme and the M-MKMS scheme.

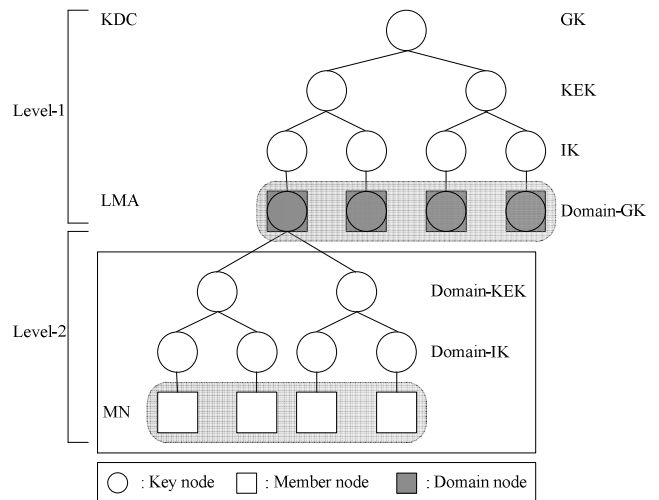


Figure 4. Key management in L-MKMS.

Moreover, in the L-MKMS method, the LMA acts as a key node and a member node at the same time.

### 3.2.1. Multicast Data Transmission

In figure 1, the SP encrypts the multicast data with the *GK* and sends to the LMA, which decrypts data with its *GK*. The LMA then encrypts the data with the domain group key (*Domain-GK*), and multicasts it to all members via the MAG-LMA tunnel. Note that the role of *Domain-GK* is similar to *GK* but it belongs to the domain in the serving range of the LMD. In addition, the relation between *GK* and *Domain-GK* is independent. Finally, the recipients use the *Domain-GK* to decrypt and obtain the data.

### 3.2.2. Join Operation

When an MN joins a group, backward secrecy must be ensured so that the new member cannot decrypt the multicast data sent before he joined. There are two possible scenarios when an MN wants to join a multicast group: (i) the LMA is not a member of the multicast group; or (ii) the LMA is

already a member. Note that the LMA does not change the *Domain-GK* when the MN hands off to a different MAG in the same serving range of the LMD. The steps of the join operation are as follows.

Step 1:  $\{mn\} \rightarrow \{lma\}$ : When an MN wants to join a multicast group, it sends a group join message to the current LMA via the MAG-LMA tunnel.

Step 2: On receipt of the join message, the LMA checks whether it is a multicast member of the group that the MN wants to join. If it is not a member, it joins the multicast group through the LKH scheme (i.e., it satisfies the backward secrecy) and obtains the *GK*. Then, the KDC broadcasts the new *GK* to all LMAs. Otherwise, the LMA performs Step 3.

Step 3:  $\{lma\} \rightarrow \{MN\}$ : The LMA generates the new *Domain-GK* via the LKH scheme for the join of the MN and broadcasts the new *Domain-GK* to all MNs belonging to its domain. Note that all *Domain-KEKs* on the key path from the new member's parent to the root are compromised and should be changed (i.e., backward secrecy).

Table 2. Comparison of communication costs.

	Join		Leave
	Multicast	Unicast	
M-MKMS	$2\log_2(L \times M) - 1, 2$	$\log_2(L \times M) + 3, 2$	$2\log_2(L \times M) + 2, 2$
L-MKMS	$2\log_2 L + 2\log_2(M \times N) - 2,$ $2\log_2(M \times N) - 1$	$\log_2 L + \log_2(M \times N) + 2,$ $\log_2(M \times N) + 1$	$2\log_2 L + 2\log_2(M \times N),$ $2\log_2(M \times N)$
LKH	$2\log_2(L \times M \times N) - 1$	$\log_2(L \times M \times N) + 1$	$2\log_2(L \times M \times N)$

Table 3. Comparison of storage costs.

	MN	KDC	LMA	MAG
M-MKMS	2	$2(L \times M) - 1$	-	$\log_2(L \times M) + N + 1$
L-MKMS	$\log_2(M \times N) + 1$	$2L - 1$	$\log_2 L + 2(M \times N)$	-
LKH	$\log_2(L \times M \times N) + 1$	$2(L \times M \times N) - 1$	-	-

Step 4:  $\{lma\} \rightarrow \{mn\}$ : The LMA encrypts the new *Domain-GK* with the new member's *Domain-IK* and sends it to the new member.

The join operation satisfies the backward secrecy because the joining MN does not know the old *GK/Domain-GK* so he/she cannot decrypt the previous data).

### 3.2.3. Leave Operation

When a member leaves the group, forward secrecy must be guaranteed to prevent the departing member decrypting subsequent data transmissions. There are also two possible scenarios when an MN leaves the multicast group: (i) there are no other multicast members in the LMA; or (ii) some multicast members are still located in the LMA. The steps of the leave operation are as follows.

Step 1:  $\{mn\} \rightarrow \{lma\}$ : When an MN decides to leave the multicast group, it sends a group leave message to the current LMA.

Step 2: On receipt of the message, the LMA checks whether there are any other members in its group. To ensure forward secrecy, the LMA updates the key tree if there are no other members in its group, and the KDC broadcasts the new *GK* to all LMAs. Otherwise, the LMA performs Step 3.

Step 3:  $\{lma\} \rightarrow \{MN\}$ : The LMA generates a new *Domain-GK*, encrypts this new *Domain-GK* with each member's *Domain-IK*, and broadcasts it to each member. Note that this broadcast message contains multiple encrypted keys. The new *Domain-GK* received by each member is encrypted with his/her *Domain-IK*.

The leave operation satisfies the forward secrecy because the leaving MN does not know the new *GK/Domain-GK* so he/she cannot decrypt the later data.

### 3.2.4. Handoff Operation

The MN does not rejoin the multicast group and change the *Domain-GK* when it moves around the same LMD. However, it still needs to be authenticated when it hands off. The steps of the handoff operation are as follows.

Step 1:  $\{mag_{new}\} \rightarrow \{mag_{old}\}$ : The new MAG sends an authentication request to the old MAG.

Step 2:  $\{mag_{old}\} \rightarrow \{mag_{new}\}$ : On receipt of the request message, the old MAG sends the MN's authentication information to the new MAG., which then verifies the MN.

Step 3: If the MN's authentication request is successful, the LMA builds a bi-directional tunnel between the MAG and the LMA, encrypts the multicast data via the *Domain-*

$GK$ , and transmits it to the MN. Otherwise, the MAG asks the LMA to generate a new *Domain-GK* to guarantee backward and the forward secrecy. Note that, the authentication process is out of scope of this work, and any public key infrastructure (PKI) authentication mechanisms can be applied to here.

### 3.3. Location Privacy Enhancement

In our scheme, the M-MKMS and L-MKMS management architectures support many famous mechanisms to improve the location privacy. In physical layer, we can use frequency-hopping spread spectrum (FHSS) or time-reversal (TR) [21] schemes to support the untraceable property.

In addition, note that PMIPv6 allows the layer 2 attachment and layer 3 address to be less tightly bound (i.e., the MN uses the same IP address when it moves around the same LMD) to reduce the possibility of being tracked by an adversary. Therefore, our scheme can mitigate the movement tracking attacks.

## 4. Performance Analysis

In the following, we compare the LKH scheme with the proposed MKMS scheme, which is comprised of M-MKMS and L-MKMS. The performance metrics are the communication cost and the storage cost. In the mobile multicast network, let  $L$  be the number of LMAs belonging to the multicast group in the network;  $M$  be the number of MAGs belonging to the multicast group within a LMD; and  $N$  be the number of multicast members in a MAG. As a result, there are  $(L \times M \times N)$  members in the network. Generally, the relation between the LMA, the MAG, and the MN is  $L < M < N$ . We set the value of parameters as follows:

$L = 1 \sim 5$ ,  $M = 10 \sim 30$  and  $N = 50 \sim 250$ . To simplify the analysis, we use a balanced binary tree to build the key tree. Thus,  $(\log_2 n)$  is the height of the tree, where  $n$  is the number of member in the group.

### 4.1. Communication Cost

The communication cost is comprised of the total number of rekeying messages transmitted per operation by the KDC, the LMA, and the MAG. We evaluate the communication costs of the join and leave operations. The communication cost of the join operation includes the unicast cost (i.e., the KDC sends the group key to new members) and the multicast cost (i.e., the KDC sends the new group key to existing members). The communication cost of the leave operation contains the whole messages sent by KDC, LMA, or MAG to notify all remaining members to update the key. Table 2 presents the communication costs of LKH, M-MKMS, and L-MKMS. Figures 5, 6, 7, and 8 depict the performance comparisons of communication cost with different parameters (i.e.,  $L$ ,  $M$ , and  $N$ ) in join procedure and Figures 9 and 10 depict the performance comparisons of communication cost with different parameters in leaving procedure.

The LKH scheme has the most communication cost since it suffers from the “one affects all” problem. In M-MKMS and L-MKMS, there are two values in the join and leave operations. The first value means that the MAG/LMA also needs to update the group key (i.e.,  $GK$ ); while the second value means that the MAG/LMA only changes the key locally (i.e., *Local-GK/Domain-GK*). As a result, we can observe that the two-level key management scheme (i.e., M-MKMS and L-MKMS) is superior to the one-level scheme (i.e., LKH).

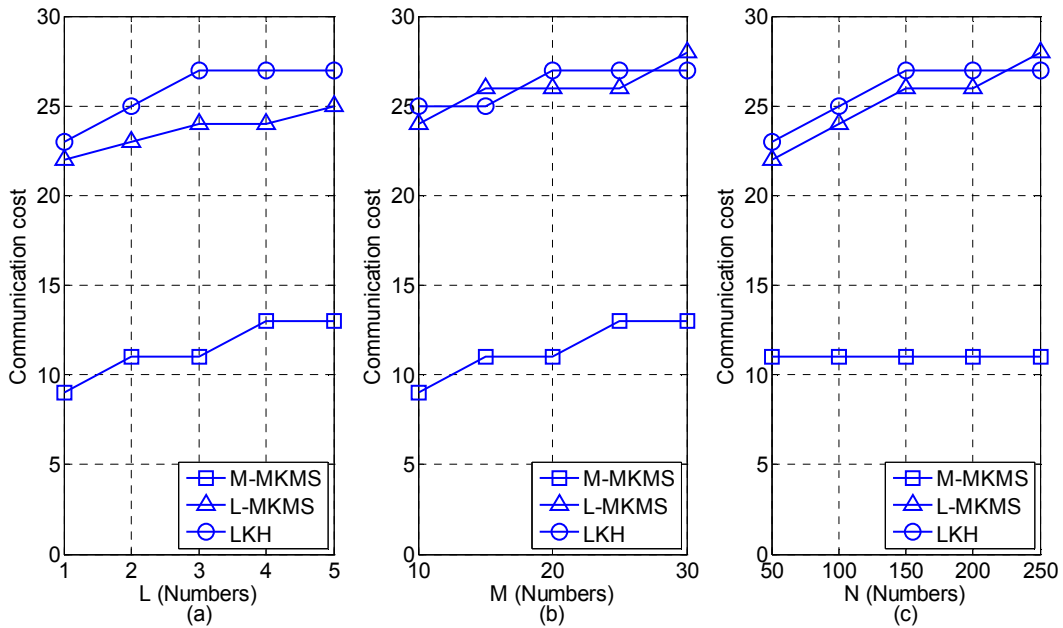


Figure 5. Performance comparisons of communication cost with different parameters in join procedure (under multicast mode and GK update situation).

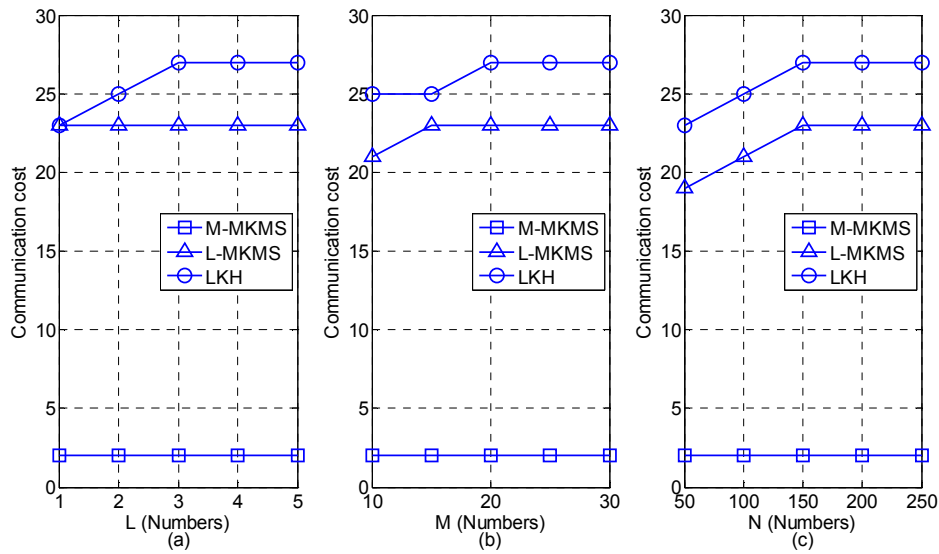


Figure 6. Performance comparisons of communication cost with different parameters in join procedure (under multicast mode and local GK update situation).

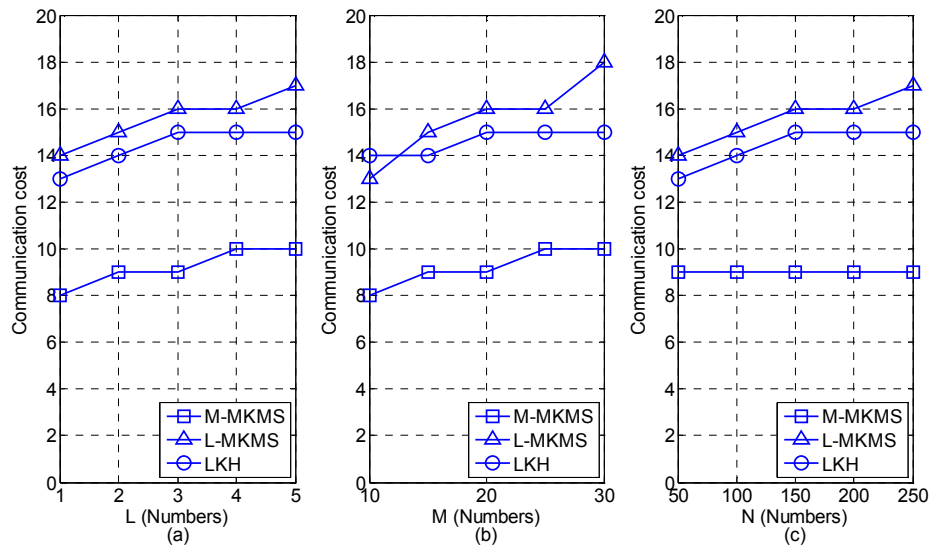


Figure 7. Performance comparisons of communication cost with different parameters in join procedure (under unicast mode and GK update situation).

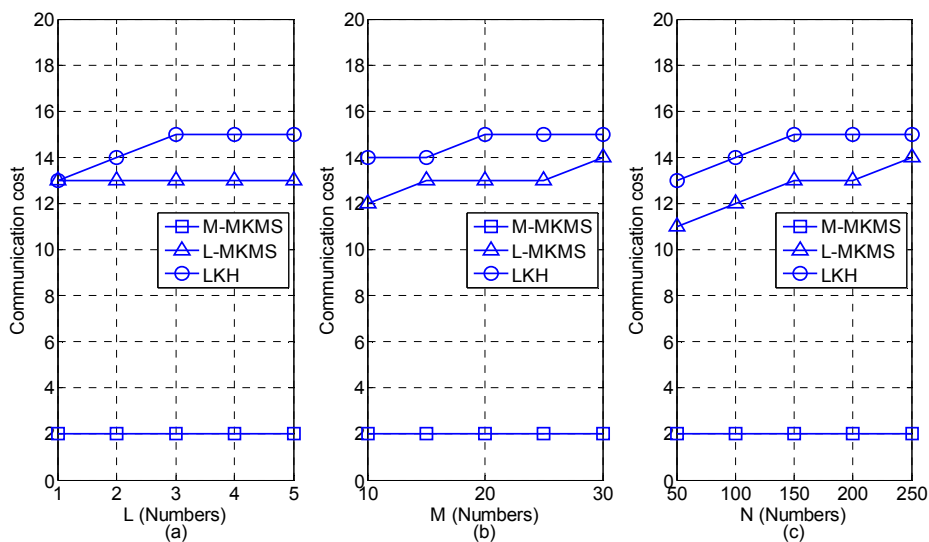


Figure 8. Performance comparisons of communication cost with different parameters in join procedure (under unicast mode and local GK update situation).



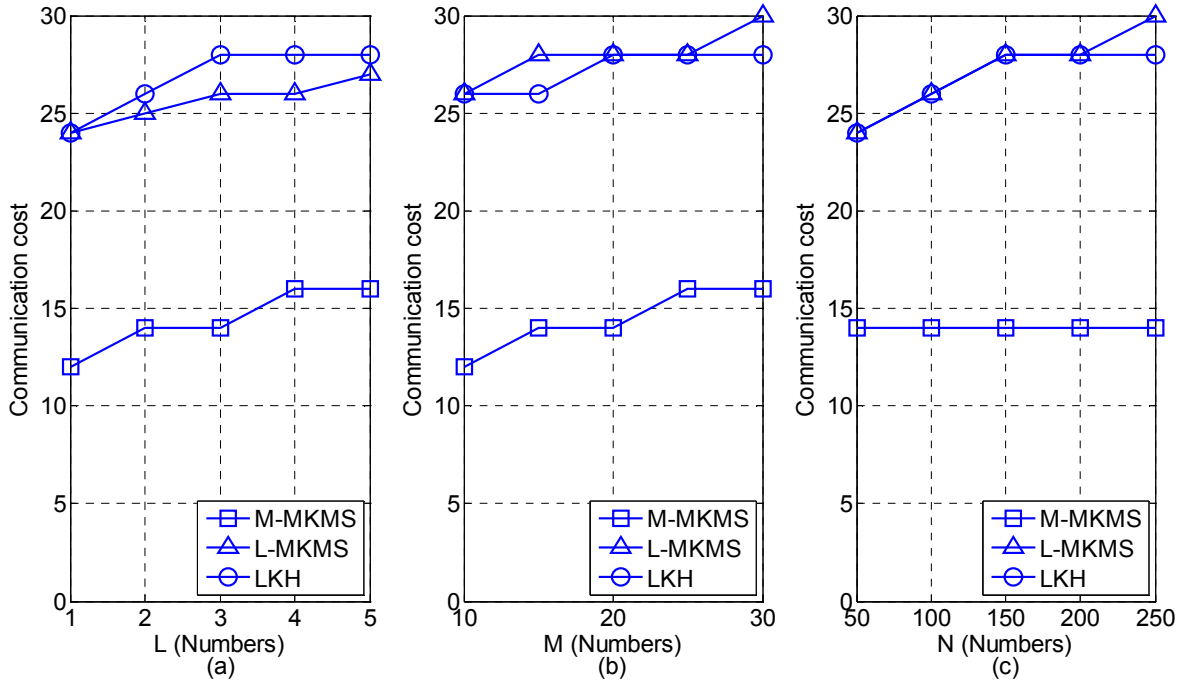


Figure 9. Performance comparisons of communication cost with different parameters in leaving procedure (GK update situation).

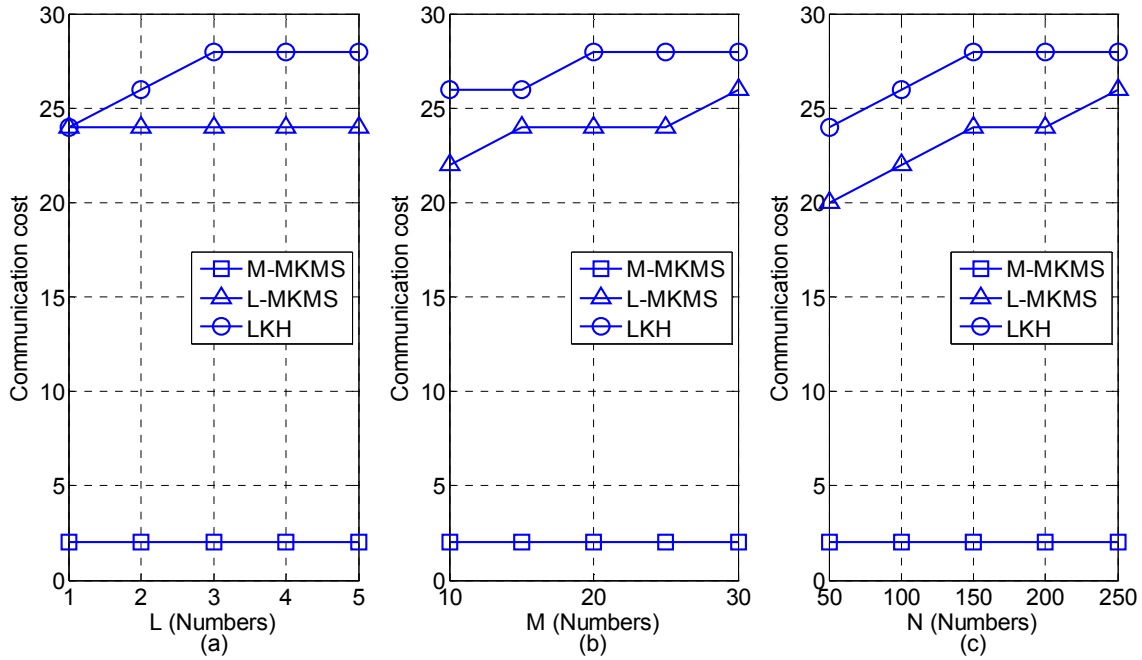


Figure 10. Performance comparisons of communication cost with different parameters in leaving procedure (local GK update situation).

#### 4.2. Storage Cost

The storage cost means that the total numbers of keys are stored in the network entities. Table 3 shows the storage costs of LKH, M-MKMS, and L-MKMS. Figures 11, 12, 13, and 14 display the comparisons of storage cost of the MN, KDC, LMA, and MAG, respectively.

The LKH scheme incurs a higher storage cost at the KDC and the MN since the KDC needs to manage the keys of all members. In addition, LKH builds a bigger key tree resulting in the key path from the leaf to the root is longer (i.e., the

MN needs more storage cost). On the contrary, we can see that both MN and KDC in our proposed mechanisms need less storage requirement than LKH scheme. In M-MKMS, the MN only needs to store the *Local-GK* and *PK* keys. Moreover, in L-MKMS, the KDC has the lowest storage cost because the scheme is based on a two-level key management architecture, so the KDC does not need to manage the keys of all members. In other words, the MAGs and LMAs can share the load of the KDC in M-MKMS and L-MKMS approaches, respectively.



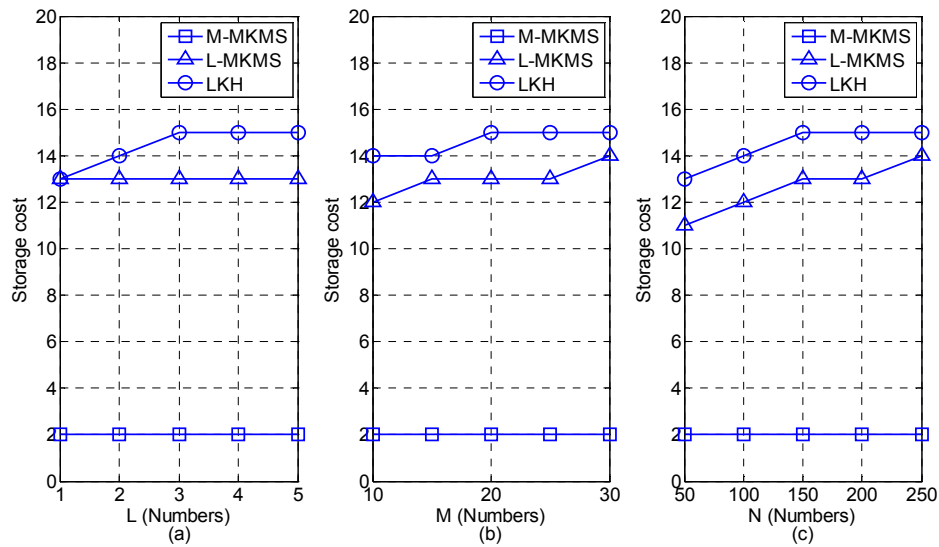


Figure 11. Performance comparisons of storage cost of the MN with different parameters.

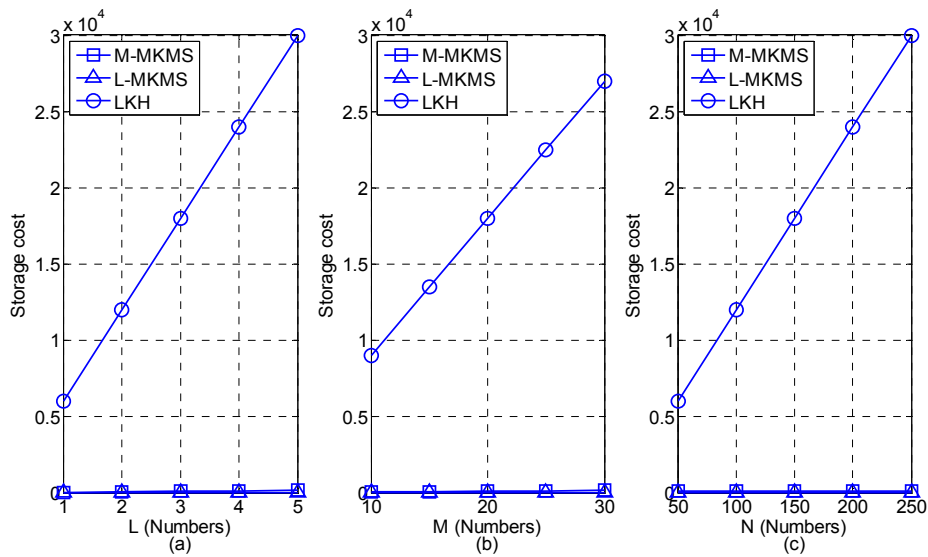


Figure 12. Performance comparisons of storage cost of the KDC with different parameters.

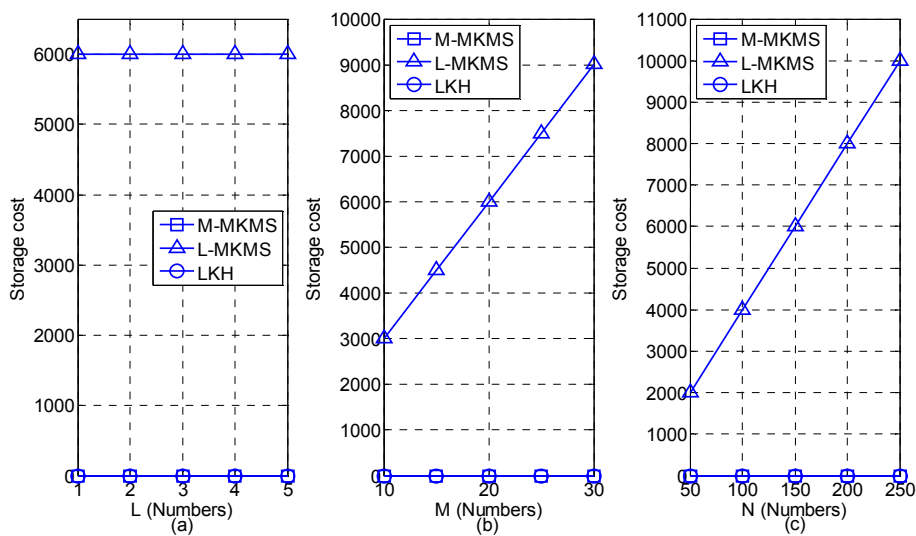


Figure 13. Performance comparisons of storage cost of the LMA with different parameters.

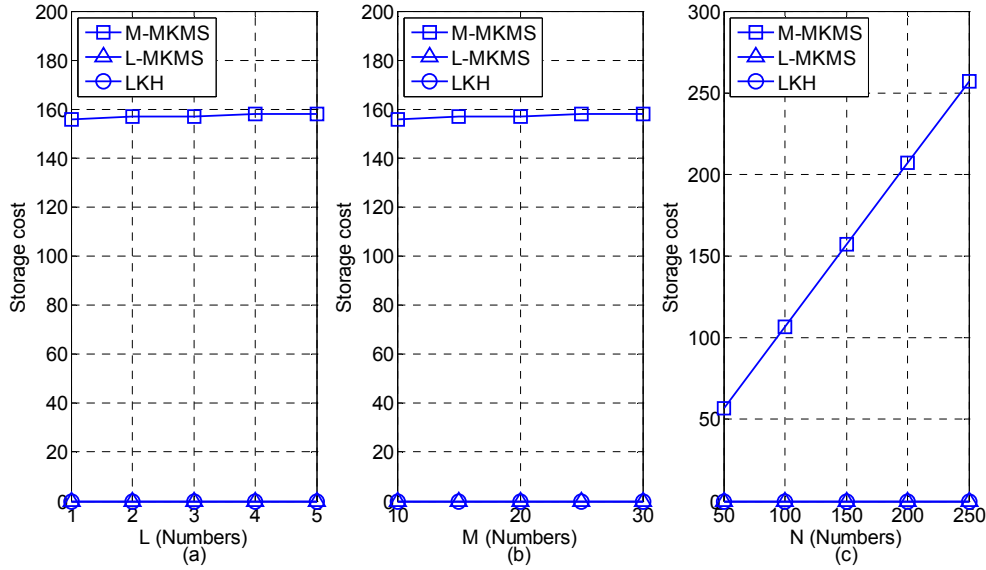


Figure 14. Performance comparisons of storage cost of the MAG with different parameters.

### 4.3. Guidelines

This section discusses the key management architecture, and then we provide some guidelines for ISPs. In communication aspect, although the M-MKMS scheme incurs the lowest communication cost, it is not necessarily the best method. For example, the join and leave operations are often performed resulting in communication cost increasing quickly when the MN moves around different MAGs frequently. In contrast, the L-MKMS method has fewer opportunities to perform join and leave operations, but the communication cost for each rekey operation is higher. Therefore, the ISP selects the suitable key management architecture to minimize the communication cost according to the MN's moving pattern. In storage aspect, the ISP needs to consider the actual hardware capacity and the deployment cost of the network entity. Consequently, the ISP chooses the M-MKMS scheme to minimize the total storage cost if it has enough funds.

## 5. Concluding Remarks

The multicast issue in future mobile communication networks has generated a great deal of interest among researchers. However, multicast key management, which is an essential constituent of network security, has not been widely addressed. In this paper, we propose two multicast key management schemes (M-MKMS and L-MKMS) for secure group communications based on LMA-based and MAG-based multicast methods in PMIPv6-based LTE networks. The schemes satisfy the forward and the backward secrecy requirement, and mitigate the "one affects all" problem in the LKH scheme with lower storage and communication costs. In the end, we give some guidelines for ISPs to select the suitable key management architecture.

## References

- [1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," *RFC 5213*, Aug. 2008.
- [2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *RFC 3775*, Jun. 2004.
- [3] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," *RFC 5380*, Oct. 2008.
- [4] Ed. R. Koodli, "Mobile IPv6 Fast Handovers," *RFC 5268*, Jun. 2008.
- [5] F. Xia and B. Sarikaya, "FMIPv6 Extension for Multicast Handover," *Draft-xia-mipshop-fmip-multicast-01*, IETF draft, Sep. 2007.
- [6] G. A. Leoleisa, G. N. Prezerakosb, and I. S. Venierisa, "Seamless Multicast Mobility Support Using Fast MIPv6 Extensions," *Computer Communications*, vol. 29, pp. 3745-3765, Nov. 2006.
- [7] D. H. Kwon, W. J. Kim, Y. S. Kim, W. S. Im, Y.J. Suh, "Design and Implementation of an Efficient Multicast Support Scheme for FMIPv6," *IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1-12, Apr. 2006.
- [8] T. C. Schmidt and M. Waehlich, "Seamless Multicast Handover in a Hierarchical Mobile IPv6 Environment (M-HMIPv6)," *Draft-schmidt-waehlich-mhmip6-04*, IETF draft, Nov. 2005.
- [9] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," *RFC 3810*, Jun. 2004.
- [10] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet Group Management Protocol, Version 3," *RFC 3376*, Oct. 2002.
- [11] J. Guan, Y. Qin, S. Gao, and H. Zhang, "The Performance Analysis of Multicast in Proxy Mobile IPv6," *IEEE International Conference on Communications Technology and Applications (ICCTA)*, pp. 719-723, Oct. 2009.

- [12] M. Hui, G. Chen, and H. Deng, "Fast Handover for Multicast in Proxy Mobile IPv6," *Draft-hui-multimob-fast-handover-00, IETF draft*, Jun. 2009.
- [13] H. Asaeda, P. Seite, and J. Xia, "PMIPv6 Extensions for Multicast," *Draft-asaeda-multimob-pmip6-extension-03, IETF draft*, Mar. 2010.
- [14] J. Guan, H. Zhou, H. Zhang, and H. Luo, "Multicast Extension Support for Proxy MIPv6," *IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 1-5, Jan. 2010.
- [15] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architecture," *RFC 2627*, Jun. 1999.
- [16] C. K. Wong, M. Gouda, and S. S. Lam, "Secure Group Communications Using Key Graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16-30, Feb. 2000.
- [17] Y. Sun, W. Trappe, and K. J. R. Liu, "An Efficient Key Management Scheme for Secure Wireless Multicast," *IEEE International Conference on Communications (ICC)*, pp. 1236-1240, Aug. 2002.
- [18] Y. Sun, W. Trappe, and K. J. R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 4, pp. 653-666, Aug. 2004.
- [19] Architecture Enhancements for Non-3GPP Accesses, 3GPP Technical Specifications TS23.402, Mar. 2008.
- [20] 3rd Generation Partnership Project TS24.312. (Dec. 2008). Access Network Discovery and Selection Function (ANDSF) Management Object (MO), Release 8, v8.0.0.
- [21] B. B. Wang, Y. L. Wu, F. Han, Y. H. Yang, and K. J. Ray Liu, "Green Wireless Communications: A Time-Reversal Paradigm," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 29, no. 8, pp. 1698-1710, Sept. 2011.
- [22] Aparna S. Pande and Ravindra. C. Thool, "Survey on Logical Key Hierarchy for Secure Group Communication," *IEEE International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, pp. 1131-1136, Sept. 2016.
- [23] Azana Hafizah Mohd Aman, Aisha-Hassan A. Hashim, Azween Abdullah, Huda Adibah Mohd, and Ramli and Shayla Islam, "Advance Signaling Cost for Multicast Fast Reroute Proxy Mobility Management," *Indian Journal of Science and Technology*, vol. 9, pp. 1-6, Jul. 2016.
- [24] Manisha Yadav, Karan Singh, and Ajay Shekhar Pandey, "Key Management in Efficient and Secure Group Communication," *IEEE International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES)*, pp. 196-203, Mar. 2016.
- [25] Yi Ren, Jyh-Cheng Chen, Jui-Chih Chin, and Yu-Chee Tseng, "Design and Analysis of the Key Management Mechanism in Evolved Multimedia Broadcast/Multicast Service," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8463-8476, Oct. 2016.