Key Management for UMTS MBMS

Shin-Ming Cheng, *Member, IEEE,* Wei-Ru Lai, *Member, IEEE,* Phone Lin, *Senior Member, IEEE,* and Kwang-Cheng Chen, *Fellow, IEEE*

***Abstract*—3GPP 33.246 proposes** *Key Management Mechanism* **(KMM) to distribute security keys for** *Universal Mobile Telecommunications System* **(UMTS)** *Multimedia Broadcast and Multicast Service* **(MBMS). KMM introduces extra communication overhead to UMTS. The previous study,** *Key-Tree Scheme* **(KTS), resolves this issue for the IP multicast network. However, this scheme may not be so efficient while applied in UMTS MBMS due to lots of storage space and heavy multicast traffic introduced, which may decrease the QoS of UMTS MBMS. In this paper, we propose a more efficient scheme,** *Hash Function Scheme* **(HFS), to release both storage and communication overhead for KMM in UMTS MBMS. We first modify the KTS applied in the UMTS MBMS and then detail the execution of HFS, which is proven to be correct. We conduct an analytical model and simulation experiments to compare the performance between the UMTS KMM with KTS and with HFS. Our study shows that the proposed HFS can reduce both communication and storage overhead without damaging QoS of UMTS MBMS.**

***Index Terms*—Hash function, key management, multimedia broadcast and multicast service (MBMS), Universal Mobile Telecommunications System (UMTS).**

I. Introduction

TO DELIVER multimedia content efficiently over the Universal Mobile Telecommunications System (UMTS), 3GPP proposed the Multimedia Broadcast/Multicast Service (MBMS) based on UMTS [1], [2]. UMTS MBMS utilizes point-to-multipoint transmission technology, where the multimedia content is delivered from a single source to a group of mobile devices through the UMTS MBMS transmission bearer.

Manuscript received April 15, 2007; revised August 15, 2007; accepted November 6, 2007. The associate editor coordinating the review of this paper and approving it for publication was W. Lou. The work of P. Lin was sponsored in part by the National Science Council (NSC), R.O.C., under the contract number NSC-96-2627-E-002-001-, NSC-96-2811-E-002-010, NSC-96-2628-E-002-002-MY2 and NSC-95-2221-E-002-091-MY3, Ministry of Economic Affairs (MOEA), R.O.C., under contract number 93-EC-17-A-05-S1-0017, Telcordia Applied Research Center, Taiwan Network Information Center (TWNIC), Excellent Research Projects of National Taiwan University, 95R0062-AE00-07, and Chunghwa telecom M-Taiwan program M-Taoyuan Porject. This paper was presented in part (titled as "A Hash Function Scheme for Key Management in UMTS MBMS") at IEEE Globecom'07, including the key tree scheme, the hash function scheme, and the security analysis. This full version extends the performance evaluation section (which includes the analytic model in Appendix A, simulation experiments, and complete performance study).

S.-M. Cheng is with the Department of Electrical Engineering, National Taiwan University, Taipei 106, Taiwan, R.O.C. (e-mail: smcheng@cc.ee.ntu.edu.tw).

W.-R. Lai is with the Department of Communications Engineering, Yuan Ze University, Tao-Yuan 320, Taiwan, R.O.C. (e-mail: wrlai@saturn.yzu.edu.tw).

P. Lin is with the Department of Computer Science & Information Engineering and Graduate Institute of Networking & Multimedia, National Taiwan University, Taipei 106, Taiwan, R.O.C. (e-mail: plin@csie.ntu.edu.tw).

K.-C. Chen is with the Department of Electrical Engineering, National Taiwan University, Taipei 106, Taiwan, R.O.C. (e-mail: chenkc@cc.ee.ntu.edu.tw).

Digital Object Identifier 10.1109/TWC.2008.070400.

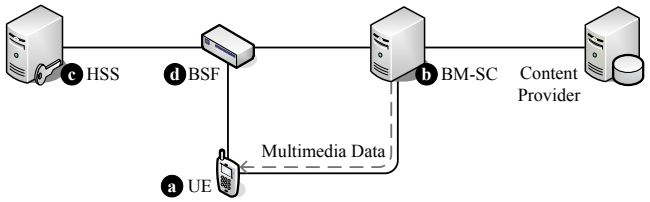


Fig. 1. A simplified UMTS MBMS network architecture.

Figure 1 illustrates the simplified UMTS MBMS network architecture [3], without showing the network elements supporting MBMS transmission bearers in UMTS. The User Equipment (UE; Figure 1 (a)) receives the MBMS application (also known as MBMS User Service) [4] from the Broadcast-Multicast Service Center (BM-SC; Figure 1 (b)), which is an application server serving as an MBMS data source or as an entry point for the multimedia content provider. The UEs joining the multicast group for a specific MBMS User Service are called joined UEs. The BM-SC initializes the establishment of the MBMS transmission bearer, then sends multimedia content to the joined UEs. The Home Subscriber Subsystem (HSS; Figure 1 (c)) maintains UMTS subscriber information (e.g., security-related information). The Bootstrapping Server Function (BSF; Figure 1 (d)) is a security server function, which is responsible for establishing shared secrets between the BM-SC and UEs.

The BM-SC multicasts MBMS content to the joined UEs via a broadcasting network bearer, where the MBMS point-to-multipoint Traffic Channel (MTCH) in the air interface [5] is used to carry the multicast content. To prevent the non-joined UEs from receiving the MBMS content, 3GPP 33.246 proposed the Key Management Mechanism (KMM) [6], which are described in detail below. A specific MBMS User Service has two corresponding group keys, namely the MBMS Transmission Key (MTK; denoted as **T**) and the MBMS Service Key (MSK; denoted as **S**). Every UE of an MBMS User Service group has the same **S** and **T**. **T** is used to protect multicast content from eavesdropping or modification, where the multicast content is encrypted by **T** before being multicasted to all joined UEs. A UE uses **T** to decrypt content that it receives. **T** is multicasted from BM-SC to all joined UEs by sending $\mathbf{S}\{\mathbf{T}\}$, which means that **T** is encrypted by **S**. **S** is individually unicasted from BM-SC to every joined UE.

During an MBMS User Service, **T** or **S** is updated when one of the following events occurs: (Event 1) a new UE joins the multicast group; (Event 2) a joined UE leaves the multicast group; (Event 3) the timer of the current **S** expires, or (Event 4) the timer of the current **T** expires. The User Service Join procedure (denoted as `P1` for Event 1), the User Service Leave procedure (denoted as `P2` for Event 2), the MSK Periodic Update procedure (denoted as `P3` for Event 3), and the MTK

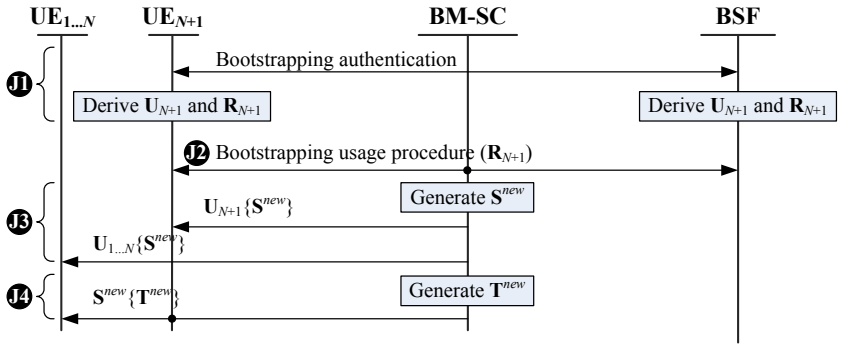


Fig. 2. Message flow for the User Service Join procedure in KMM.

Periodic Update procedure (denoted as P4 for Event 4) are exercised at this moment in order to update **T** or **S** [6]. The four procedures are described in detail below.

Figure 2 shows the message flow for Procedure P1 with the following steps, where we suppose that the multicast group contains N joined UEs. Assume that a new UE, UE_{N+1}, joins the MBMS User Service, and before UE_{N+1} joins the service, the two keys, $\mathbf{S}^{old}$ and $\mathbf{T}^{old}$ are used for the MBMS User Service.

User Service Join Procedure P1:

Step J1. UE_{N+1} performs the bootstrapping authentication procedure [3] with BSF to obtain an MBMS Request Key (denoted as $\mathbf{R}_{N+1}$) and an MBMS User Key (denoted as $\mathbf{U}_{N+1}$).

Step J2. UE_{N+1} uses $\mathbf{R}_{N+1}$ as the authentication password when executing the bootstrapping usage procedure [3] with BM-SC and BSF.

Step J3. If the authentication in Step J2 is successful, then BM-SC generates $\mathbf{S}^{new}$, and unicasts it to every UE, UE_i, in the multicast group by sending $\mathbf{U}_i\{\mathbf{S}^{new}\}$. Otherwise (i.e., the authentication fails), the procedure quits. This step requires $N+1$ unicasts to deliver $\mathbf{S}^{new}$.

Step J4. BM-SC generates $\mathbf{T}^{new}$, and multicasts it to all joined UEs by sending $\mathbf{S}^{new}\{\mathbf{T}^{new}\}$. Significantly, only one multicast transmission is necessary.

The other three procedures are similar to Procedure P1. Procedure P2 consists of three steps, Steps L1–L3, which are the same as Steps J2–J4, respectively. Procedure P3 comprises two steps, Steps S1 and S2, which are the same as Steps J3 and J4, respectively. Procedure P4 consists of only one step, Step T1, which is the same as Step J4.

Note that in Step J3, **S** is unicasted through the Dedicated Control Channel (DCCH), which is a signaling message. Conversely, in Step J4, **T** is multicasted using the MIKEY protocol [7], and **T** is delivered via the MTCH, which is used to carry the multimedia content and other session information. In other words, **T** delivery may consume the radio resource for the transmission of multicast content. This study considers the following two main issues.

Issue 1. The number of unicast key deliveries should be minimized to lower signaling overhead.

Issue 2. The number of multicast key deliveries should be minimized to provide an acceptable QoS (i.e., more bandwidth can be used to transmit multicast content).

Only one group key (that is used for data encryption and unicasted to every member of a multicast group) is defined in IP multicast networks. Previous studies [8]–[11] have attempted to reduce the number of unicastings for the group key deliveries in IP multicast networks by proposing *Key-Tree Scheme* (KTS), which applies multicast Key Encryption Keys (KEKs; cf. Section II) to all members of a multicast group. The KTS was applied in cellular networks in 2004 [12], [13], when the UMTS MBMS has not been well defined (i.e., only one group key was considered in these studies).

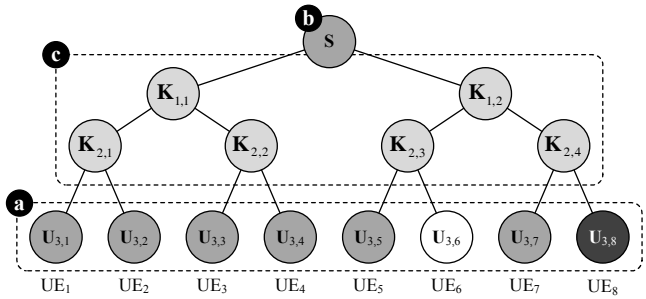


Fig. 3. An example of the key tree in KTS.

In this work, to consider Issues 1 and 2, KTS is first modified so that it can be applied in UMTS MBMS KMM. Analytical results indicate that KTS is not efficient in UMTS MBMS KMM. The *Hash Function Scheme* (HFS), which is regarded as more efficient than KTS, is then proposed. The rest of this paper is organized as follows. The application of KTS in the existing UMTS MBMS KMM is described in Section II. Section III details HFS. Section IV provides security analysis for HFS. Section V conducts an analytical model and simulation experiments to evaluate the performance of KMM with/without KTS or HFS. Finally, Section VI concludes this work.

II. KTS IN UMTS MBMS KEY MANAGEMENT

This section describes how to apply KTS in UMTS MBMS KMM. In KTS, BM-SC establishes and maintains a balanced binary key tree [8], [9]. As shown in Figure 3, each leaf **U** of the tree is assigned to corresponding joined UE (Figure 3 (a)). The root of the key tree is **S** for the multicast group (Figure 3 (b)). The intermediate nodes of the key tree are the intermediate KEKs (Figure 3 (c)), which are used to facilitate efficient **S** updates.

Consider N joined UEs, UE_1, UE_2, ..., UE_N, in the multicast group. Let H be the height of the binary tree, which

can be calculated by $H = \lceil \lg N \rceil$. The keys in the tree have the index number (i, j), where $0 \le i < H$ is the layer number, and $1 \le j \le 2^i$ is the position number in layer i. The index number for the parent of the KEK with the index (i, j) is given by $(i-1, \lceil \frac{j}{2} \rceil)$. Suppose that UE_j is assigned the user key $\mathbf{U}_{H,j}$ where $1 \le j \le N$. The content is encrypted by the intermediate key $\mathbf{K}_{i,j}$ before it is multicasted to 2^{H-i} UEs, $\text{UE}_{2^{H-i}(j-1)+1}$, $\text{UE}_{2^{H-i}(j-1)+2}$, ..., $\text{UE}_{2^{H-i}j}$. $\mathbf{U}_{H,j}$ is used to encrypt the key that will be unicasted to UE_j. UE_j stores $\mathbf{S}$, $\mathbf{T}$, $\mathbf{R}_j$, $\mathbf{U}_{H,j}$ and $H-1$ intermediate keys, $\mathbf{K}_{H-1,\lceil \frac{j}{2} \rceil}$, $\mathbf{K}_{H-2,\lceil \frac{j}{2^2} \rceil}$, ..., $\mathbf{K}_{1,\lceil \frac{j}{2^{H-1}} \rceil}$. In other words, UE_j contains $H+3$ keys.

In the original KMM in UMTS, the new $\mathbf{S}$ should be unicasted to all joined UEs to update an old $\mathbf{S}$. In KTS, the multicast technology can be applied to deliver the new $\mathbf{S}$. Consider Figure 3 as an example. To deliver a new $\mathbf{S}$ to UE_1, UE_2, ..., UE_8, BM-SC can multicast $\mathbf{K}_{1,1}\{\mathbf{S}^{new}\}$ to UE_1, UE_2, UE_3, UE_4 and multicast $\mathbf{K}_{1,2}\{\mathbf{S}^{new}\}$ to UE_5, UE_6, UE_7, UE_8. To apply KTS in KMM, Procedure `P4` is not modified, while the other three procedures are modified as follows:

User Service Leave Procedure `P2`**:** The Steps L1 and L3 are the same as those in KMM while the Step L2 is modified as follows. Assume that UE_l leaves the multicast group. The group keys (including $\mathbf{S}$ and $H-1$ KEKs) known by UE_l should be updated so that UE_l cannot decode any future multicast content. $\mathbf{K}^{old}_{H-1,\lceil \frac{l}{2} \rceil}$ is updated to $\mathbf{K}^{new}_{H-1,\lceil \frac{l}{2} \rceil}$; $\mathbf{K}^{old}_{H-2,\lceil \frac{l}{2^2} \rceil}$ is updated to $\mathbf{K}^{new}_{H-2,\lceil \frac{l}{2^2} \rceil}$; ...; $\mathbf{K}^{old}_{1,\lceil \frac{l}{2^{H-1}} \rceil}$ is updated to $\mathbf{K}^{new}_{1,\lceil \frac{l}{2^{H-1}} \rceil}$, and $\mathbf{S}^{old}$ is updated to $\mathbf{S}^{new}$. All newly generated keys should be delivered to all joined UEs that own the old keys. The following actions are taken. The KEK, $\mathbf{K}^{new}_{H-1,\lceil \frac{l}{2} \rceil}$, is unicasted to the other UE that owns $\mathbf{K}^{old}_{H-1,\lceil \frac{l}{2} \rceil}$ (i.e., UE_{l+1} if l is odd, or UE_{l-1} if l is even). $\mathbf{K}^{new}_{H-2,\lceil \frac{l}{2^2} \rceil}$, ..., $\mathbf{K}^{new}_{1,\lceil \frac{l}{2^{H-1}} \rceil}$ and $\mathbf{S}^{new}$ are multicasted to the UEs that own the old keys, and are encrypted with each of their respective children's KEKs. Take Figure 3 as an example. Originally, there are 7 joined UEs, UE_1, UE_2, ..., UE_7, and later UE_6 leaves the multicast group. In this case, the following four steps are exercised in Step L2.

- **Step L2-1.** The BM-SC updates the two old KEKs, $\mathbf{K}^{old}_{1,2}$ and $\mathbf{K}^{old}_{2,3}$ as $\mathbf{K}^{new}_{1,2}$ and $\mathbf{K}^{new}_{2,3}$ and the old MSK $\mathbf{S}^{old}$ as $\mathbf{S}^{new}$ for UE_5 by unicasting $\mathbf{U}_{3,5}\{\mathbf{K}^{new}_{1,2}, \mathbf{K}^{new}_{2,3}, \mathbf{S}^{new}\}$ to UE_5.
- **Step L2-2.** The BM-SC updates the old KEK $\mathbf{K}^{old}_{1,2}$ as $\mathbf{K}^{new}_{1,2}$ for UE_7 by multicasting $\mathbf{K}^{old}_{2,4}\{\mathbf{K}^{new}_{1,2}\}$ to UE_7.
- **Step L2-3.** The BM-SC updates the old MSK $\mathbf{S}^{old}$ as $\mathbf{S}^{new}$ for UE_1, UE_2, ..., UE_4 by multicasting $\mathbf{K}_{1,1}\{\mathbf{S}^{new}\}$ to UE_1, UE_2, UE_3 and UE_4.
- **Step L2-4.** The BM-SC updates the old MSK $\mathbf{S}^{old}$ as $\mathbf{S}^{new}$ for UE_5 and UE_7 by multicasting $\mathbf{K}^{new}_{1,2}\{\mathbf{S}^{new}\}$ to UE_5 and UE_7.

Note that the key tree may not be balanced when a UE leaves. As recommended by Moyer et al. [14], the key tree should be regenerated by running the Re-balance algorithm. After the key tree regeneration, the newly generated keys should be delivered to the affected joined UEs. As noted in [14], the number of keys that need to be updated is twice that in a non-balanced key tree after a UE leaves.

User Service Join Procedure `P1`**:** When a new UE, UE′, joins the multicast group, the BM-SC first determines the corresponding $\mathbf{U}$ position in the key tree for UE′ by executing the Re-balance algorithm in [14]. Let k be the position number of the found $\mathbf{U}$ position, i.e., UE′ is assigned $\mathbf{U}_{H,k}$. To simplify our description, UE′ is denoted as UE_k hereafter.

To prevent UE_k from decoding overheard multicast content, $\mathbf{K}^{old}_{H-1,\lceil \frac{k}{2} \rceil}$, $\mathbf{K}^{old}_{H-2,\lceil \frac{k}{2^2} \rceil}$, ..., $\mathbf{K}^{old}_{1,\lceil \frac{k}{2^{H-1}} \rceil}$ and $\mathbf{S}^{old}$ should be updated. The newly generated keys (i.e., $\mathbf{K}^{new}_{H-1,\lceil \frac{k}{2} \rceil}$, $\mathbf{K}^{new}_{H-2,\lceil \frac{k}{2^2} \rceil}$, ..., $\mathbf{K}^{new}_{1,\lceil \frac{k}{2^{H-1}} \rceil}$ and $\mathbf{S}^{new}$) are delivered to all joined UEs that own the old keys, which are encrypted by the old keys. BM-SC then unicasts $\mathbf{U}_{H,k}\{\mathbf{K}^{new}_{H-1,\lceil \frac{k}{2} \rceil}, \mathbf{K}^{new}_{H-2,\lceil \frac{k}{2^2} \rceil}, ..., \mathbf{K}^{new}_{1,\lceil \frac{k}{2^{H-1}} \rceil}, \mathbf{S}^{new}\}$ to UE_k. In the example of Figure 3, where UE_8 joins the multicast group, BM-SC multicasts $\mathbf{K}^{old}_{1,2}\{\mathbf{K}^{new}_{1,2}\}$ to UE_5, UE_6 and UE_7, and unicasts $\mathbf{U}_{3,8}\{\mathbf{K}^{new}_{2,4}, \mathbf{K}^{new}_{1,2}, \mathbf{S}^{new}\}$ to UE_8, in order to deliver $\mathbf{K}^{new}_{1,2}$ to UE_5, UE_6, UE_7 and UE_8. These key deliveries are performed at Step J3.

MSK Update Procedure `P3`**:** To update $\mathbf{S}$, the all KEKs and $\mathbf{S}$ in the key tree should be regenerated and unicast to all joined UEs, including $\mathbf{S}$ and $H-1$ KEKs. The key deliveries can be performed at Step S1.

In KTS, delivery of intermediate KEKs requires multicast transmission. According to the UMTS KMM, KEKs may be delivered through the MTCH. Based on the UMTS MBMS standard [4], the following two implementation methods are available for KEK delivery: (i) BM-SC creates a new multicast group for the KEK delivery, and (ii) BM-SC multicasts KEKs through the network bearer of the original multicast group. In method (i), to form a new multicast group, all joined UEs should perform the MBMS Multicast Service Activation procedure [2], which incurs heavy signaling overhead to the UMTS network. Method (ii) is thus more practical than method (i). However, method (ii) consumes radio resource (carrying the multicast content) in delivering KEKs, thus decreasing the QoS of multicast content. Furthermore, KTS has the following problems.

- In KTS, $H+3$ keys are stored in a UE. Increasing the number of joined UEs (i.e., increasing H) raises the amount of storage space required, and therefore may not be practical due to the limited UE storage space.
- KTS may require much extra key transmission overhead to keep the key tree balanced when UEs join or leave.

The next section proposes the Hash Function Scheme (HFS) for KMM in UMTS MBMS by utilizing the one-way hash function to resolve both Issues 1 and 2 without extra storage space.

III. Hash Function Scheme

A one-way hash function $h(\cdot)$ is a powerful and computationally efficient cryptographic tool [15], which takes a message of arbitrary size as its input, and outputs a fixed string. "One way" means that the original input cannot feasibly

be derived from the output. The one-way property of hash function is utilized to update **S** efficiently. The idea of HFS is that BM-SC requests (through multicast) UEs to generate a new **S** by using $h(\cdot)$ instead of unicast **S** to all UEs. The HFS exercises as follows. Suppose that the multicast group contains N joined UEs, namely UE_1, UE_2, ..., UE_N, and $\mathbf{S}^{old}$ and $\mathbf{T}^{old}$ are used for the MBMS User Service. To apply HFS to KMM, Procedures `P1` and `P3` are modified as follows, while the other two procedures (`P2` and `P4`) remain the same as those in KMM.

User Service Join Procedure `P1`**:** Figure 4 shows the message flow for this procedure, where Steps J1 and J2 are the same as that in KMM, and Steps J3 and J4 are modified. Assume that a UE, UE_{N+1}, joins the multicast group. If $N = 0$ (i.e., UE_{N+1} is the only user in the multicast group), then this procedure is the same as that in KMM of MBMS UMTS. For $N > 0$, UE_{N+1} is assigned $\mathbf{U}_{N+1}$ after being successfully authenticated. The BM-SC generates a new **T**, $\mathbf{T}^{new}$ and a new **S** by executing $\mathbf{S}^{new} = h(\mathbf{T}^{new}, \mathbf{S}^{old})$. Then BM-SC unicasts $\mathbf{U}_{N+1}\{\mathbf{S}^{new}, \mathbf{T}^{new}\}$ to UE_{N+1}. Then BM-SC multicasts $\mathbf{S}^{old}\{\mathbf{T}^{new}\}$ to the other N joined UEs. The N UEs generate $\mathbf{S}^{new}$ by executing $\mathbf{S}^{new} = h(\mathbf{T}^{new}, \mathbf{S}^{old})$, respectively.

MSK Update Procedure `P3`**:** The BM-SC generates a new **T**, $\mathbf{T}^{new}$ and a new **S** by executing $\mathbf{S}^{new} = h(\mathbf{T}^{new}, \mathbf{S}^{old})$. Then, BM-SC multicasts $\mathbf{S}^{old}\{\mathbf{T}^{new}\}$ to N joined UEs. The N UEs generate $\mathbf{S}^{new}$ by executing $\mathbf{S}^{new} = h(\mathbf{T}^{new}, \mathbf{S}^{old})$, respectively.

The SHA-1 [16] (the standard one-way hash function installed in the UE) can be utilized to implement HFS. The implementation cost of HFS is considered insignificant. For the robustness of SHA-1, as mentioned in [15], theoretically, it requires 2^{80} trials using the brute-force method to break the full 80-step SHA-1, which is considered big overhead. In the recent studies [15], [17], the birthday attack and multicollision attack were proposed to break SHA with less

computation overhead, whose details can be found in [15], [17]. Wang et al. [18] reduced the complexity of the computation (to find a collision in SHA-1 using collision search attack) to 2^{69}. The computation overhead is still high, i.e., up to several hours. In HFS, the one-way hash function $h(\cdot)$ is applied when only Event 1 or 3 occurs. For Events 2 and 4, HFS follows the standard procedures in MBMS KMM. Usually, the time interval between the occurrence of Event 2 and the occurrence of Event 4 is shorter than one hour. In other words, before SHA-1 is broken, UE may retrieve new **S** and **T** from BM-SC. Thus, HFS is considered robust under birthday and multicollision attacks.

IV. Security Analysis

A secured multicast mechanism should satisfy the group secrecy property [19], which stipulates the following requirements.

- *Nongroup confidentiality*: only the joined UEs can decode the multicast content, i.e., non-joined UEs cannot decode it.
- *Forward secrecy*: a UE joining at time t cannot decode any multicast content before t.
- *Backward secrecy*: a UE leaving at time t cannot decode any multicast content after t.

This section analyzes the group secrecy property for the KMM, KMM with KTS (denoted as $\mathrm{KMM_{KTS}}$), and KMM with HFS (denoted as $\mathrm{KMM_{HFS}}$).

As specified in [6], in KMM, nongroup confidentiality can be achieved by group keys **S** and **T**, and forward and backward confidentialities can be achieved via Procedures `P1` and `P2`, respectively. Additionally, in [8], $\mathrm{KMM_{KTS}}$ has been proven to be able to achieve the three confidentialities. In $\mathrm{KMM_{HFS}}$, Procedure `P2` is the same as that in KMM, and backward secrecy can be achieved. In $\mathrm{KMM_{HFS}}$, we modify Procedures `P1` and `P3` in KMM. In $\mathrm{KMM_{HFS}}$, Procedure `P1` is invoked to update **S** and **T** when a new UE joins the multicast group at t. Since the UE does not have the old **T** and **S**, it cannot decode any content multicasted before t, and forward secrecy holds in $\mathrm{KMM_{HFS}}$.

In KMM, **T** is used to encode the multicast content for security protection, and **S** is used to encrypt the multicast transmission of **T**. The following lemma proves that HFS prevents any malicious UE from obtaining **S** and **T**, and therefore cannot steal the multicast content. In other words, $\mathrm{KMM_{HFS}}$ holds nongroup confidentiality.

Lemma1 1: Let t_i be the time when the ith event occurs during a multicast session, and $\mathbf{S}^{(i)}$ and $\mathbf{T}^{(i)}$ denote **S** and **T** used at the ith event. Suppose that a malicious UE, UE_m, starts to overhear the multicast information at time t' during the period between t_i and t_{i+1}, i.e., $t_i \leq t' < t_{i+1}$. Then with $\mathrm{KMM_{HFS}}$, UE_m cannot get $\mathbf{S}^{(i)}$ and $\mathbf{T}^{(i)}$.

Proof: The proof is completed by considering the following two conditions.

Condition 1: $t' > t_i$**.** The multicast information (overheard by UE_m during the time period $[t'\ t_{i+1})$) is $\mathbf{T}^{(i)}\{\text{content}\}$, and UE_m cannot retrieve $\mathbf{S}^{(i)}$ and $\mathbf{T}^{(i)}$ from this information.

Condition 2: $t' = t_i$**.** During the time period $[t_i\ t_{i+1})$, UE_m can overhear $\mathbf{S}^{(i)}\{\mathbf{T}^{(i)}\}$ and $\mathbf{T}^{(i)}\{\text{content}\}$. In this condition, if UE_m cannot get $\mathbf{S}^{(i)}$, then he cannot steal the content. Hypothesis "*UE_m cannot get* $\mathbf{S}^{(i)}$" is proven to hold by induction on i.

Basic: If $i = 1$ in KMM, then the ith event must be Event 1. The first UE joins the multicast group, and $\mathbf{S}^{(1)}$ is unicasted with protection to this UE. The UE_m cannot obtain $\mathbf{S}^{(1)}$, and the hypothesis holds.

Inductive Step: Suppose that the hypothesis holds when $i = k$ (i.e., UE_m cannot get $\mathbf{S}^{(k)}$). For $i = k + 1$, consider the following four cases:

Case 1: The $k + 1$st event is Event 1. At t_{k+1}, all joined UEs respectively generate $\mathbf{S}^{(k+1)}$ by executing Procedure `P1` in $\mathrm{KMM_{HFS}}$, and have

$$\mathbf{S}^{(k+1)} = h(\mathbf{T}^{(k+1)}, \mathbf{S}^{(k)}) \tag{1}$$

where $\mathbf{T}^{(k+1)}$ is delivered by multicast $\mathbf{S}^{(k)}\{\mathbf{T}^{(k+1)}\}$. Since UE_m cannot obtain $\mathbf{S}^{(k)}$, he cannot retrieve $\mathbf{S}^{(k+1)}$.

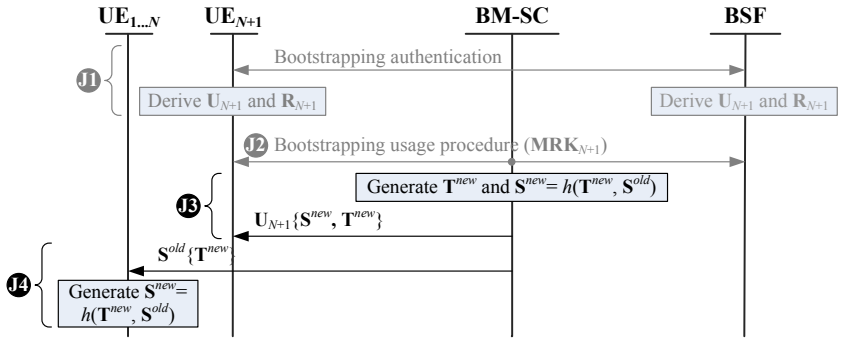


Fig. 4. Message flow for the User Service Join procedure in HFS.

Case 2: The $k+1$st event is Event 2. At t_{k+1}, $\mathbf{S}^{(k+1)}$ is unicasted with protection to all joined UEs by BM-SC (see Procedure P2 in KMM_{HFS}), and thus UE_m cannot get $\mathbf{S}^{(k+1)}$.

Case 3: The $k+1$st event is Event 3. At t_{k+1}, all joined UEs respectively generate $\mathbf{S}^{(k+1)}$ by executing Procedure P3 in KMM_{HFS} using (1). In the same reason mentioned in Case 1, UE_m cannot get $\mathbf{S}^{(k+1)}$.

Case 4: The $k+1$st event is Event 4. At t_{k+1}, all joined UEs update $\mathbf{T}$ by receiving the multicasted $\mathbf{S}^{(k+1)}\{\mathbf{T}^{(k+1)}\}$ from BM-SC (see Procedure P4 in KMM_{HFS}), and $\mathbf{S}^{(k+1)}$ is the same as $\mathbf{S}^{(k)}$. Since UE_m cannot obtain $\mathbf{S}^{(k)}$, $\mathbf{S}^{(k+1)}$ cannot be retrieved by UE_m.

Thus, the hypothesis holds for all cases.

■

V. Performance Evaluation

This study develops an analytic model and simulation experiments to investigate the performance for KMM, KMM_{KTS} and KMM_{HFS}. Appendix A describes the analytic model in details. The simulation model adopts the event-driven approach widely used in mobile network studies [20]. Both models are validated against each other in Appendix A. More than 500,000 experiments are executed to ensure the stability of the simulation results.

In this study, the session time T_s of an MBMS User Service session is modeled as a widely used Gamma distribution with mean $\frac{1}{\mu}$ and variance v_s [20] because Gamma distribution can be shaped to represent many distributions, as well as to measure data that cannot be characterized by a particular distribution [21]. Additionally, this distribution has been widely used in mobile network studies [20]. A UE may join or leave the multicast group during an MBMS User Service session. Assume that the UE inter-arrival time t_a to an MBMS User Service session has Gamma distribution with mean $\frac{1}{\lambda}$ and variance v_a. The resident time t_u (when the joined UE stays in an MBMS User Service session) is assumed to be Gamma distributed with mean $\frac{1}{\eta}$ and variance $v_u = \frac{1}{\alpha\eta^2}$, where α is the shape parameter. During an MBMS User Service session, $\mathbf{S}$ and $\mathbf{T}$ are periodically updated every Δ_s and Δ_t time units, respectively. The other notations used in this study include the random number N (to count the number of current joined UEs in a multicast group at a specific time point), the total number X of UEs that have joined the multicast group during the period T_s and the total number Y of UEs that have left the multicast group during the period T_s.

This study applies videos as multicast sessions to investigate the performance of MBMS User Services. The average session time ($\frac{1}{\mu}$) is 100 mins, and the variance of session time (v_s) is 570 min^2. If v_s is large (e.g., $v_s \geq \frac{1}{\mu^2}$), then most of generated session times are very small numbers (the curve of Gamma density function can be found in Figure 11 of Chapter 3 [21]) and not fit to represent the periods of movies. Therefore, a small variance is chosen to approximate the real world. According to Chebyshev's Inequality, the probability P that the session times are out of the range $[\frac{1}{\mu}-t, \frac{1}{\mu}+t]$ is less than $\frac{v_s}{t^2}$ for all t. If $\frac{1}{\mu} = 100$ mins and $v_s = 570$ min^2, then P is less than 63.3%. The numerical results indicate that P is about 20%. Furthermore, the effects of $\frac{1}{\lambda}$, v_a and $\frac{1}{\eta}$ (discussed later) are similar even for different v_s. Therefore, the performance results specifically for Exponential session times are not presented. For the same reason, $\alpha = 4$ is chosen for the Gamma resident time t_u so that a reasonable number of UEs stay in the MBMS service within any time period. Anyway, it is easy to adjust these parameters to simulate different behaviors of MBMS services.

Let e_i be the number of Events i ($i = 1, 2, 3$ or 4) occurring in a multicast session. Let $N_{i,j}$ be the number of joined UEs in the multicast group at the jth occurrence of Event i. As specified in [6], $\mathbf{T}$ and $\mathbf{S}$ have the same size of 128 bits. Let $n_{u,i}(N_{i,j})$ and $n_{m,i}(N_{i,j})$, be the numbers of unicast and multicast messages used to deliver $\mathbf{S}$ or $\mathbf{T}$ at the jth occurrence of Event i conditioning on there are $N_{i,j}$ joined UEs, respectively. Let $k_{u,i}(N_{i,j})$ and $k_{m,i}(N_{i,j})$ be the numbers of keys ($\mathbf{T}$ or $\mathbf{S}$) carried in a unicast and a multicast messages at the jth occurrence of Event i conditioning on there are $N_{i,j}$ joined UEs, respectively. Let $s_{u,i}(N_{i,j})$ and $s_{m,i}(N_{i,j})$ be the total number of keys ($\mathbf{S}$ or $\mathbf{T}$) carried in unicast and multicast messages at the jth occurrence of Event i conditioning on there are $N_{i,j}$ joined UEs, respectively. For $i = 1, 2, 3, 4$, we have $s_{u,i}(N_{i,j}) = n_{u,i}(N_{i,j})k_{u,i}(N_{i,j})$ and $s_{m,i}(N_{i,j}) = n_{m,i}(N_{i,j})k_{m,i}(N_{i,j})$. Figure 5 lists the $n_{u,i}(N_{i,j})$, $n_{m,i}(N_{i,j})$, $k_{u,i}(N_{i,j})$, $k_{m,i}(N_{i,j})$, $s_{u,i}(N_{i,j})$, and $s_{m,i}(N_{i,j})$ values for KMM, KMM_{KTS}, and KMM_{HFS}, where $i = 1, 2, 3, 4$. Note that the analysis for KMM_{KTS} in Figure 5 is simplified due to the complexity of key tree regeneration. This study investigates the following output measures.

	KMM						KMM_{HFS}					
	$n_{u,i}(N_{i,j})$	$n_{m,i}(N_{i,j})$	$k_{u,i}(N_{i,j})$	$k_{m,i}(N_{i,j})$	$s_{u,i}(N_{i,j})$	$s_{m,i}(N_{i,j})$	$n_{u,i}(N_{i,j})$	$n_{m,i}(N_{i,j})$	$k_{u,i}(N_{i,j})$	$k_{m,i}(N_{i,j})$	$s_{u,i}(N_{i,j})$	$s_{m,i}(N_{i,j})$
i=1	$N_{1,j}$+1	1	1	1	$N_{1,j}$+1	1	1	1	2	1	2	1
i=2	$N_{2,j}$−1	1	1	1	$N_{2,j}$−1	1	$N_{2,j}$−1	1	1	1	$N_{2,j}$−1	1
i=3	$N_{3,j}$	1	1	1	$N_{3,j}$	1	0	1	0	1	0	1
i=4	0	1	0	1	0	1	0	1	0	1	0	1
	KMM_{KTS}											
	$n_{u,i}(N_{i,j})$	$n_{m,i}(N_{i,j})$		$k_{u,i}(N_{i,j})$	$k_{m,i}(N_{i,j})$	$s_{u,i}(N_{i,j})$		$s_{m,i}(N_{i,j})$				
i=1	1	$\lceil \lg(N_{1,j}+1) \rceil + 1$		$\lceil \lg(N_{1,j}+1) \rceil$	1	$\lceil \lg(N_{1,j}+1) \rceil$		$\lceil \lg(N_{1,j}+1) \rceil + 1$				
i=2	1	$2\lceil \lg(N_{2,j}-1) \rceil - 1$		$\lceil \lg(N_{2,j}-1) \rceil$	1	$\lceil \lg(N_{2,j}-1) \rceil$		$2\lceil \lg(N_{2,j}-1) \rceil - 1$				
i=3	$N_{3,j}$	1		$\lceil \lg N_{3,j} \rceil$	1	$N_{3,j}\lceil \lg N_{3,j} \rceil$		1				
i=4	0	1		0	1	0		1				

Fig. 5. $n_{u,i}(N_{i,j})$, $n_{m,i}(N_{i,j})$, $k_{u,i}(N_{i,j})$, $k_{m,i}(N_{i,j})$, $s_{u,i}(N_{i,j})$, and $s_{m,i}(N_{i,j})$ values for $i = 1, 2, 3, 4$ in KMM, KMM_{KTS}, and KMM_{HFS}.

- M_u or M_m: the numbers of unicast or multicast messages used to deliver **S** or **T** during a multicast session, which is calculated as

$$M_u = \sum_{i=1}^{4}\sum_{j=1}^{e_i} n_{u,i}(N_{i,j}) \quad \text{or} \quad M_m = \sum_{i=1}^{4}\sum_{j=1}^{e_i} n_{m,i}(N_{i,j}). \quad (2)$$

- S_u or S_m: the total number of keys (**S** or **T**) carried in unicast or multicast messages during a multicast session, which is obtained as follows

$$S_u = \sum_{i=1}^{4}\sum_{j=1}^{e_i} s_{u,i}(N_{i,j}) \quad \text{or} \quad S_m = \sum_{i=1}^{4}\sum_{j=1}^{e_i} s_{m,i}(N_{i,j}). \quad (3)$$

(2), (3) and Figure 5 clearly indicate that $M_m = S_m$ for each scheme, since every multicast message contains only one key, i.e., $k_{m,1}(N_{1,j}) = k_{m,2}(N_{2,j}) = k_{m,3}(N_{3,j}) = k_{m,4}(N_{4,j}) = 1$ for all j. Additionally, KMM and KMM_{HFS} have the same M_m values. Based on the simulation experiments, the impacts of the input parameters on the output measures are elaborated as follows.

Effects of $\frac{1}{\lambda}$: Figure 6 plots M_u, S_u and S_m as functions of $\frac{1}{\lambda}$ for KMM, KMM_{KTS} and KMM_{HFS}, where $\frac{1}{\mu} = 100$ mins, $v_s = 570$ min^2, $\frac{1}{\eta} = 60$ mins, $\alpha = 4$, $\Delta_t = 5$ mins and $\Delta_s = 20$ mins. The inter-arrival time is exponentially distributed with mean $\frac{1}{\lambda}$ mins.

The figure shows an intuitive result that M_u, S_u and S_m decrease as $\frac{1}{\lambda}$ increases. A lower $\frac{1}{\lambda}$ implies that more UEs join (i.e., a larger X), stay (i.e., a larger N) and then leave (i.e., a larger Y) the service. Based on Figure 5, explicitly all of M_u, S_u and S_m are decreasing functions when $\frac{1}{\lambda}$ increases.

Figure 6 (a) indicates that decreasing $\frac{1}{\lambda}$ significantly increases M_u of KMM and slightly increases M_u of KMM_{HFS}. Decreasing $\frac{1}{\lambda}$ only insignificantly affects M_u of KMM_{KTS}. In KMM, BM-SC needs to unicast **S** to all UEs in service at Procedures `P1`, `P2` and `P3`, and the effort of **S** delivery is large if the net traffic is heavy. In KMM_{HFS}, **S** is delivered to all UEs at Procedure `P2`, and thus the M_u of KMM_{HFS} is smaller than that of KMM. In KMM_{KTS}, only for Procedure `P3`, BM-SC unicasts **S** to all UEs while `P3` rarely executes. Thus, M_u of KMM_{KTS} is insensitive to the change in $\frac{1}{\lambda}$, and is the smallest among the three schemes.

Since the wireless bandwidth is precious, the total number of keys carried in unicast/multicast messages is calculated to find the bandwidth consumed for each of the three schemes. Figure 6 (b) shows the total number of keys carried in unicast messages for the three schemes. The figure indicates when the traffic is small (i.e., $\frac{1}{\lambda} \geq 1.4$ mins), the S_u of KMM_{HFS} is less than that of KMM_{KTS}. Conversely, when the traffic is large (i.e., $\frac{1}{\lambda} < 1.4$ mins), KMM_{KTS} requires fewer keys to deliver than KMM_{HFS}. As $\frac{1}{\lambda}$ decreases, N and Y increase, and therefore S_u of KMM_{HFS} increases rapidly since the number of unicast messages for Procedure `P2` is $O(N)$. For KMM_{KTS}, the keys of each unicast message at `P1`, `P2` and `P3` is $O(\lg N)$ and S_u of KMM_{KTS} increases slowly. If N is small, then KMM_{HFS} has a smaller S_u than KMM_{KTS}. When the net traffic is heavy, the gap between $O(N)$ and $O(\lg N)$ increases rapidly, and KMM_{KTS} performs better than the other two schemes.

Figure 6 (c) shows that as $\frac{1}{\lambda}$ decreases, S_m of KMM_{KTS} increases more rapidly than that of KMM and KMM_{HFS}. Note that $S_m = M_m$ for each scheme individually, and S_m are the same for KMM and KMM_{HFS}. Since the number of keys carried in each multicast message at Procedures `P1` and `P2` is $O(\lg N)$, S_m of KMM_{KTS} increases rapidly as $\frac{1}{\lambda}$ decreases.

All of the multicast messages for KMM_{KTS} are used for key distribution, and must be transmitted in real-time. Consider a special scenario in which many UEs join or depart simultaneously during a short period. Since `P1` and `P2` need to transmit many keys, and occupy the MTCH, the multimedia content is likely to be compressed, thus degrading QoS. Although KMM_{KTS} has better performance for **Issue 1**, the requirement of **Issue 2** is not guaranteed.

Effects of v_a: Figure 7 plot S_u and S_m as functions of v_a for KMM, KMM_{HFS} and KMM_{KTS}, respectively. In these figures, $\frac{1}{\lambda} = 2$ mins, $\frac{1}{\mu} = 100$ mins, $v_s = 570$ min^2, $\frac{1}{\eta} = 60$ mins, $\alpha = 4$, $\Delta_t = 5$ mins and $\Delta_s = 20$ mins. Note that if the variance (v_a) equals to 4 min^2, then the inter-arrival times form an Exponential distribution, and S_u and S_m for KMM_{HFS} are smaller than those of KMM_{KTS}, as revealed in Figure 6. We observe the following.

- For $v_a < 1$ min^2, S_u and S_m are insensitive to the variance of the inter-arrival time.
- For $v_a \geq 1$ min^2, S_u and S_m are increasing functions of v_a. Specifically, a change in v_a significantly affects S_u of KMM and KMM_{HFS}.

A large v_a means the system traffic becomes more bursty, that is, most inter-arrival times are very small, but a few of them are very large. The inter-arrival times thus diverge in a wide range. If the same period T_s is observed, then the number of UEs joining the service (i.e., X) for a large v_a is greater than that for
a small v_a, and the effect of increasing v_a is similar to the effect of decreasing $\frac{1}{\lambda}$. Therefore, S_u and S_m increase as v_a increases. Specifically, if $v_a \geq 60$ min^2, the S_u of KMM_{HFS} is larger than that of KMM_{KTS}.

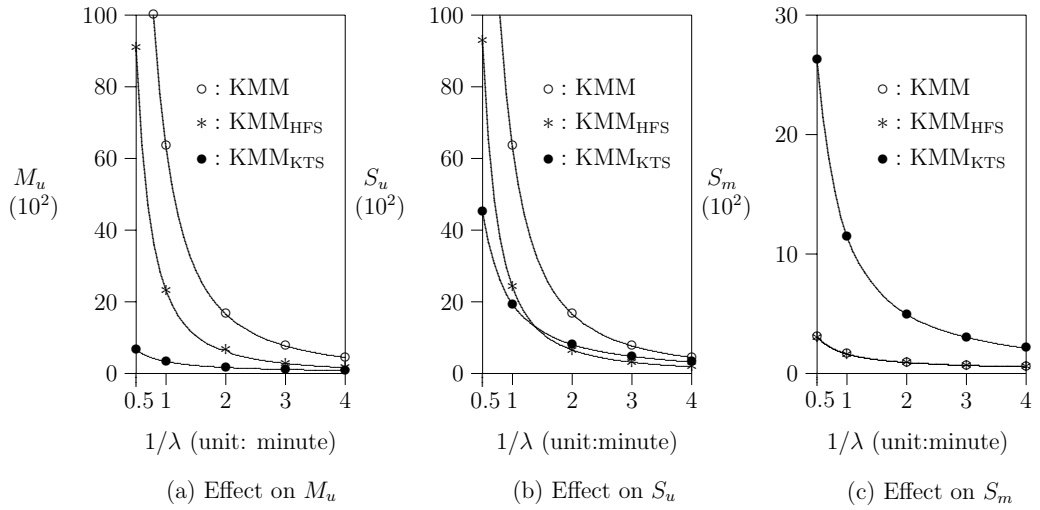


Fig. 6. The effects of $\frac{1}{\lambda}$ on M_u, S_u, S_m and M_m ($\frac{1}{\mu} = 100$ mins; $v_s = 570$ min^2; $\frac{1}{\eta} = 60$ mins; $\alpha = 4$; $\Delta_t = 5$ mins; $\Delta_s = 20$ mins).

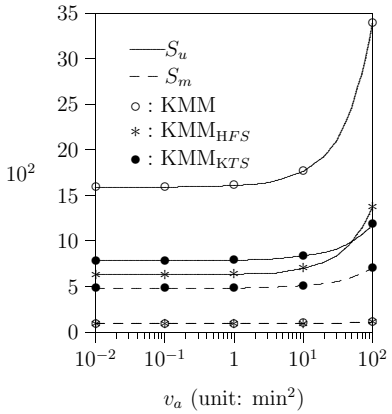


Fig. 7. The effects of v_a on S_u and S_m ($\frac{1}{\lambda} = 2$ mins; $\frac{1}{\mu} = 100$ mins; $v_s = 570$ min^2; $\frac{1}{\eta} = 60$ mins; $\alpha = 4$; $\Delta_t = 5$ mins; $\Delta_s = 20$ mins).

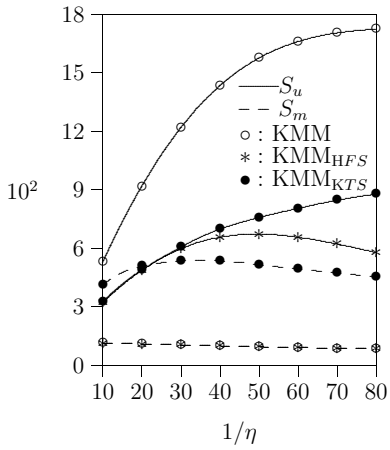


Fig. 8. The effects of $\frac{1}{\eta}$ on S_u and S_m ($\frac{1}{\lambda} = 2$ mins; $v_a = 4$ min^2; $\frac{1}{\mu} = 100$ mins; $v_s = 570$ min^2; $\alpha = 4$; $\Delta_t = 5$ mins; $\Delta_s = 20$ mins).

Effects of $\frac{1}{\eta}$: Figure 8 plots S_u and S_m as functions of the mean session holding time $\frac{1}{\eta}$ for KMM, KMM$_{\rm KTS}$ and KMM$_{\rm HFS}$, respectively. In these figures, $\frac{1}{\lambda} = 2$ mins, $v_a = 4$ min^2, $\alpha = 4$, $\frac{1}{\mu} = 100$ mins , $v_s = 570$ min^2, $\Delta_t = 5$ mins and $\Delta_s = 20$ mins. Notably, X is fixed for every $\frac{1}{\eta}$, and the execution numbers of Procedures P3 and P4 are also fixed. As $\frac{1}{\eta}$ rises (i.e., the time period that a joined UE remains in the service rises), Y falls and N rises. Since the total traffic to the system is fixed, increasing $\frac{1}{\eta}$ has the following phenomena.

- **Phenomenon 1:** As $\frac{1}{\eta}$ increases, Y decreases linearly, which implies that the execution number of Procedure P2 of the three schemes decreases.
- **Phenomenon 2:** As $\frac{1}{\eta}$ increases, N increases, which implies that the number of unicast messages for each Procedure P2 of KMM and KMM$_{\rm HFS}$ increases.
- **Phenomenon 3:** As $\frac{1}{\eta}$ increases, N increases, which implies that the number of unicast messages for each Procedure P1 of KMM increases.
- **Phenomenon 4:** As $\frac{1}{\eta}$ increases, N increases, which implies that the number of unicast messages for each Procedure P3 of KMM and KMM$_{\rm KTS}$ increases.
- **Phenomenon 5:** As $\frac{1}{\eta}$ increases, N increases, indicating that the number of keys carried in each unicast message for Procedures P1, P2 and P3 of KMM$_{\rm KTS}$ increases.
- **Phenomenon 6:** As $\frac{1}{\eta}$ increases, N increases, indicating that the number of multicast messages for each Procedures P1 or P2 of KMM$_{\rm KTS}$ increases.

The interaction between Phenomena 1 and 2 is subtle. For KMM$_{\rm HFS}$, the total number of unicast messages triggered by the departure procedures first increases and then decreases as $\frac{1}{\eta}$ increases, as does S_u. The interaction effect for KMM is similar to that of KMM$_{HFS}$. However, due to Phenomena 3 and 4, the S_u of KMM increases as $\frac{1}{\eta}$ increases. For KMM$_{\rm KTS}$, the effect of Phenomena 1, 4 and 5 interact, causing S_u to increase slowly as $\frac{1}{\eta}$ increases.

Due to Phenomenon 1, S_m of KMM and KMM$_{\rm HFS}$ fall as $\frac{1}{\eta}$ rises. For KMM$_{\rm KTS}$, the interaction of Phenomena 1 and 6 causes S_m to first rise and then fall as $\frac{1}{\eta}$ rises.

VI. Conclusion

This study proposed a new scheme for distributing MBMS keys over the UMTS network. Based on the concept of Key Management Mechanism (KMM) proposed by 3GPP, the Key-Tree Scheme (KMM_{KTS}), which works efficiently in wired IP networks, has been modified to fit the mobile environment. Additionally, this study proposed a new scheme, known as a Hash Function Scheme (KMM_{HFS}), in which a hash function is adopted to update the keys **S** on UEs and the BM-SC. Via the security analysis, we proved the security of KMM_{HFS}.

Simulation experiments have been developed to investigate the performance for KMM, KMM_{KTS} and KMM_{HFS}. We discussed the number of unicast/multicast messages and the number of keys sent on the unicast/multicast channels. Simulation results indicate that KMM_{HFS} needs less unicast communication than the other two schemes on S_u and S_m if the traffic is not heavy. When the number of UE arrivals is very large, KMM_{KTS} can reduce the unicast burden (i.e., S_u) but increase the multicast overhead (i.e., S_m). The burst multicast overhead due to the key distribution of KMM_{KTS} may result in that the QoS is not guaranteed in some period with very heavy traffic.

Besides, all UEs listening to the MTCH has to process every received multicast key, where the total computation overhead in all UEs increases. We should notice that the effects of multicast key delivery is more significant than the unicast key delivery. Additionally, KMM_{KTS} requires large memory in UEs. The number of group keys required for a service is $\lg N$, and it increases as more UEs join this service, while only one **S** is stored for each service in KMM and KMM_{HFS}. Thus, KMM_{KTS} is more complex than the other two schemes. By contrast, KMM and KMM_{HFS} are simple to implement. Compared with KMM, the proposed scheme KMM_{HFS} can reduce overhead in unicast messages, and also provides the same QoS, because KMM_{HFS} does not increase the multicast overhead.

Appendix A
The Analytical Model

This section proposes an analytical model to validate the simulation model by calculating the number of occurrences of executions for `P1` or `P2` during a MBMS session. Consider the timing diagram in Figure 9. Suppose that the elapse time of an MBMS User Service session, T_s, is exponentially distributed with the density function $f(t)$, the mean $\frac{1}{\mu}$ and Laplace transform $f^*(s) = \left(\frac{\mu}{\mu+s}\right)$, to validate the simulation model (which is mainly used to conduct our study and is easily applied different distributions for the session times).

During an MBMS User Service session, when an UE joins or leaves the multicast group of this service at his own will, `P1` or `P2` is triggered. In our analytical model, the UE inter-arrival time for an MBMS User Service session, t_a, is assumed to be exponentially distributed with the mean $\frac{1}{\lambda}$. The time period when the joined UE stays in the MBMS User Service session, t_u, has the density function $f_u(\cdot)$, the mean $\frac{1}{\eta}$ and the Laplace transform $f_u^*(s)$.

Let X be the number of UEs joining the multicast group conditioning the period T_s. From [22], the probability that $X = x$ during period $T_s = t$ can be expressed as

$$\Pr[X = x | T_s = t] = \frac{(\lambda t)^x}{x!} e^{-\lambda t}.$$

Then, $\Pr[X = x]$ (the probability that x UEs join the multicast group during period T_s) can be obtained as follows:

$$\begin{aligned}
\Pr[X = x] &= \int_{t=0}^{\infty} \Pr[X = x | T = t] f(t) dt \\
&= \left(\frac{\lambda^x}{x!}\right) \int_{t=0}^{\infty} t^x f(t) e^{-\lambda t} dt \\
&= \left(\frac{\lambda^x}{x!}\right) \left[(-1)^x \frac{d^x}{ds^x} f^*(s)\right]\Big|_{s=\lambda} \\
&= \frac{\mu \lambda^x}{(\mu+\lambda)^{x+1}}
\end{aligned}$$

and the expected number of X is given as

$$E[X] = \sum_{x=1}^{\infty} x \Pr[X = x] = \frac{\lambda}{\mu}. \tag{4}$$

The UEs joining the MBMS User Service within the period T_s may leave the multicast group at any time. Let τ be the time period

between the time when the UE joins the multicast group and the time when the session for the service stops. Then from [22], the density function $r(\tau)$ for the distribution of τ is expressed

$$r(\tau) = \mu \int_{t=\tau}^{\infty} f(t) = \mu[1 - F(t)]\Big|_{t=\tau}$$

where $F(t)$ is the distribution function of T_s. Since T_s is exponentially distributed, τ and T_s have the same distribution, that is $r(\tau) = \mu e^{-\mu\tau}$.

If the UE leaves the multicast group of the service before the session stops (i.e., $t_u < \tau$), the User Service Leave procedure is executed and **S** is updated. Otherwise (i.e, $t_u \geq \tau$), the current **S** remains. Let Y be the number of UEs leaving the multicast group during the period T_s. Then, $\Pr[Y = y | X = x]$ is the probability that among x joined UEs, y UEs leave (where $y \leq x$) the multicast group before the session terminates. $\Pr[Y = y | X = x]$ can be computed by counting all possible ways of y UEs leaving the multicast group before the session terminates, which is given by

$$\Pr[Y = y | X = x] = \binom{x}{y} (\Pr[t_u < \tau])^y (\Pr[t_u \geq \tau])^{x-y}. \tag{5}$$

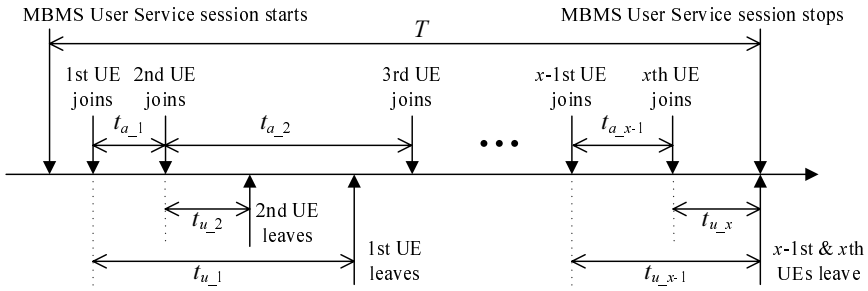
where $\Pr[t_u \geq \tau]$ can be calculated as

$$\begin{aligned}
\Pr[t_u \geq \tau] &= \int_{t_u=0}^{\infty} \int_{\tau=0}^{t_u} \mu e^{-\mu\tau} d\tau f_u(t_u) dt_u \\
&= \int_{t_u=0}^{\infty} (1 - e^{-\mu t_u}) f_u(t_u) dt_u \\
&= 1 - \int_{t_u=0}^{\infty} f_u(t_u) e^{-\mu t_u} dt_u \\
&= 1 - f_u^*(\mu),
\end{aligned} \tag{6}$$

and $\Pr[t_u < \tau]$ can be calculated as $f_u^*(\mu)$.

Thus, (5) is rewritten as

$$\Pr[Y = y | X = x] = \binom{x}{y} f_u^*(\mu)^y \left[1 - f_u^*(\mu)\right]^{x-y}.$$



t_{a_i} : the UE inter-arrival time between the ith UE and i+1st UE.

t_{u_i} : the time period when the ith joined UE stays in the session.

T : the time period for an MBMS User Service session.

Fig. 9. Timing diagram.

The expected number of Y is thus expressed as

$$\begin{aligned} E[Y] &= \sum_{x=1}^{\infty}\sum_{y=1}^{x}\{y\Pr[Y=y|X=x]\Pr[X=x]\} \\ &= \sum_{x=1}^{\infty}\left\{\left\{\sum_{y=1}^{x} y\binom{x}{y} f_u^*(\mu)^y\left[1-f_u^*(\mu)\right]^{x-y}\right\}\right. \\ &\times \left.\left[\frac{\mu\lambda^x}{(\mu+\lambda)^{x+1}}\right]\right\}. \end{aligned} \tag{7}$$

This study takes the Gamma distribution as an example for the distribution of t_u. The Gamma distribution with shape parameter α, the mean $\frac{1}{\eta}$ and the variance $v_u = \frac{1}{\alpha\eta^2}$ has the Laplace transform $f_u^*(s)$ as

$$f_u^*(s) = \left(\frac{\alpha\eta}{\alpha\eta+s}\right)^{\alpha}. \tag{8}$$

Applying (8) to (7), (7) can be written as

$$\begin{aligned} E[Y] &= \sum_{x=1}^{\infty}\left\{\left\{\sum_{y=1}^{x} y\binom{x}{y}\left(\frac{\alpha\eta}{\alpha\eta+\mu}\right)^{\alpha y}\right.\right. \\ &\times \left.\left.\left[1-\left(\frac{\alpha\eta}{\alpha\eta+\mu}\right)^{\alpha}\right]^{x-y}\right\}\left[\frac{\mu\lambda^x}{(\mu+\lambda)^{x+1}}\right]\right\}. \end{aligned} \tag{9}$$

Figure 10 plots $E[Y]$ where $T_s = 100$ and $\frac{1}{\lambda} = 4$. In this figure, solid curves are the analytical results and the points are the simulation results. The curves and the symbol points show that the analytic analysis is consistent with the simulation results (all errors are within 3%).

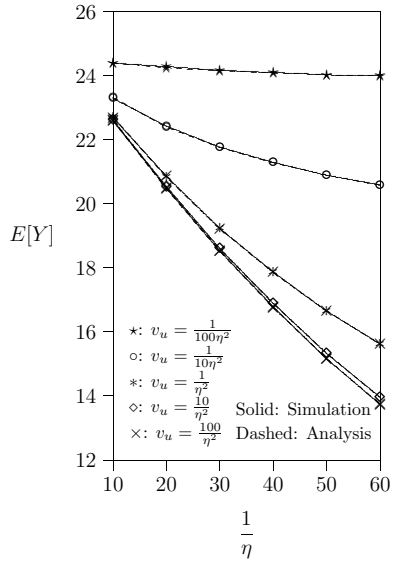


Fig. 10. Comparison between the analytic and simulation results.

ACKNOWLEDGMENT

The authors would like to thank the four anonymous reviewers. Their comments have significantly improved the quality of this paper.

REFERENCES

[1] 3GPP, "Multimedia Broadcast/Multicast Service (MBMS); Stage 1 (Release 7)," 3GPP, Tech. Rep. 3G TS 22.146 V7.1.0, Mar. 2006.

[2] ——, "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 6)," 3GPP, Tech. Rep. 3G TS 23.246 V6.10.0, June 2006.

[3] ——, "Generic Authentication Architecture (GAA); Generic bootstrapping architecture (Release 7)," 3GPP, Tech. Rep. 3G TS 33.220 V7.4.0, June 2006.

[4] ——, "Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1 (Release 8)," 3GPP, Tech. Rep. 3G TS 22.246 V8.0.0, June 2006.

[5] ——, "Radio Interface Protocol Architecture (Release 7)," 3GPP, Tech. Rep. 3G TS 25.301 V7.0.0, Apr. 2006.

[6] ——, "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (Release 7)," 3GPP, Tech. Rep. 3G TS 33.246 V7.0.0, June 2006.

[7] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing," RFC 3830, Aug. 2004.

[8] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," in *Proc. IEEE INFOCOM'99*, vol. 2, Mar. 1999, pp. 708–716.

[9] M. J. Moyer, J. R. Rao, and P. Rohatgi, "A survey of security issues in multicast communications," *IEEE Network*, vol. 13, no. 6, pp. 12–23, Nov.-Dec. 1999.

[10] D. Wallner, E. Harder, and R. Agee, "Key management for multicast: issues and architectures," RFC 2627, June 1999.

[11] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Networking*, vol. 8, no. 1, pp. 16–30, Feb. 2000.

[12] W. Xu, W. Trappe, and S. Paul, "Key management for 3G MBMS security," in *Proc. IEEE GLOBECOM'01*, vol. 4, Dec. 2004, pp. 2276–2280.

[13] Y. Sun, W. Trappe, and K. J. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," *IEEE/ACM Trans. Networking*, vol. 12, no. 4, pp. 653–666, Aug. 2004.

[14] M. J. Moyer, J. R. Rao, and P. Rohatgi, "Maintaining balanced key trees for secure multicast," IETF Draft, June 1999.
[15] A. Joux, "Collisions for SHA-0," in *rump session of Proc. CRYPTO'04*, Aug. 2004.
[16] NIST, "FIPS PUB 180-1: Secure Hash Standard," Apr. 1995.
[17] M. Nandi and D. R. Stinson, "Multicollision attacks on some generalized sequential hash functions," *IEEE Trans. Inform. Theory*, vol. 53, no. 2, pp. 759–767, Feb. 2007.
[18] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Proc. CRYPTO'05*, Aug. 2005.
[19] H. Lu, "A novel high-order tree for secure multicast key management," *IEEE Trans. Comput.*, vol. 54, no. 2, pp. 214–224, Feb. 2005.
[20] Y.-B. Lin, "Performance modeling for mobile telephone networks," *IEEE Network*, vol. 11, no. 6, pp. 63–68, Nov.-Dec. 1997.
[21] A. M. Mood, F. A. Graybill, and D. C. Boes, *Introduction to the Theory of Statistics*. McGraw-Hill Publishing Co., 1974.
[22] L. Kleinrock, *Theory, Volume 1, Queueing Systems*. Wiley-Interscience, 1975.

Shin-Ming Cheng received the BS and Ph.D. degrees in computer science and information engineering from National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively. Currently, he is a postdoctoral researcher at the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan. His research interests include mobile networking, wireless communications, and network security.

Wei-Ru Lai received the BSEE and Ph.D. degrees from the Department of computer Science and Information Engineering, National Chiao Tung University, Taiwan, R.O.C., in 1991 and 1999, respectively. In 1999, she became an Assistant Professor with the Department of Information Management, Chin-Min College, Taiwan. She is currently an Assistant Professor with the Communications Engineering Department, Yuan Ze University, Tao-Yuan, Taiwan, R.O.C. Her research interests include the design and analysis of personal communications services.

Phone Lin (M'02-SM'06) received his BSCSIE degree and Ph.D. degree from National Chiao Tung University, Taiwan, R.O.C. in 1996 and 2001, respectively. From August 2001 to July 2004, he was an Assistant Professor in Department of Computer Science and Information Engineering (CSIE), National Taiwan University, R.O.C. Since August 2004, he has been an Associate Professor in Department of CSIE and in Graduate Institute of Networking and Multimedia, National Taiwan University, R.O.C. His current research interests include personal communications services, wireless Internet, and performance modeling. Dr. Lin has published more than twenty international SCI journal papers (most of which are IEEE Transactions and ACM papers). Dr. Lin is an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, a Guest Editor for IEEE WIRELESS COMMUNICATIONS special issue on Mobility and Resource Management, and a Guest Editor for ACM/SPRINGER MONET special issue on Wireless Broad Access. He is also an Associate Editorial Member for the WCMC Journal. Dr. Lin has received many research awards. He was elected as the Best Young Researcher, the 3rd IEEE ComSoc Asia-Pacific Young Researcher Award, 2007. He was a recipient of Research Award for Young Researchers from Pan Wen-Yuan Foundation in Taiwan in 2004, a recipient of K. T. Li Young Researcher Award honored by ACM Taipei Chapter in 2004, a recipient of Wu Ta You Memorial Award of National Science Council (NSC) in Taiwan in 2005, a recipient of Fu Suu-Nien Award of NTU in 2005 for his research achievements, and a recipient of 2006 Young Electrical Engineering Award, the Chinese Institute of Electrical Engineering. Dr. Lin is listed in *Who'S Who in Science and Engineering*(R) in 2006. Dr. Lin is a Senior Member, IEEE. P. Lin's email and website addresses are plin@csie.ntu.edu.tw and http://www.csie.ntu.edu.tw/∼plin, respectively.

Kwang-Cheng Chen received B.S. from the National Taiwan University in 1983, M.S. and Ph.D. from the University of Maryland, College Park, United States, in 1987 and 1989, all in electrical engineering. From 1987 to 1998, Dr. Chen worked with SSE, COMSAT, IBM Thomas J. Watson Research Center, and National Tsing Hua University in mobile communication networks and related research. Dr. Chen is the Distinguished Professor and Irwin T. Ho Chair Professor at the Institute of Communication Engineering and Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, ROC. He holds several visiting positions with Technical University of Delft in Netherlands, HP Labs. in US, Aalborg University in Denmark. Dr. Chen actively involves the technical organization of numerous leading IEEE conferences, including 1996 IEEE International Symposium on Personal Indoor Mobile Radio Communications, IEEE Globecom 2002, 2007 IEEE Mobile WiMAX Symposium, and IEEE Vehicular Technology Conference Spring 2010. He has served editorship with many prestigious international journals: IEEE TRANSACTION ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS, IEEE JOURNAL ON SELECTED AREA IN COMMUNICATIONS, ACM/BLATZER JOURNAL ON WIRELESS NETWORKS, WIRELESS PERSONAL COMMUNICATIONS, and FRONTIERS OF COMMUNICATIONS AND INFORMATION THEORY, etc. Dr. Chen has authored and co-authored over 200 technical papers and documents, 18 granted US patents, and two books: *Mobile WiMAX*, published by Wiley in 2008, and *Principles of Communications*, published by River in 2008. Dr. Chen is an IEEE Fellow, and the recipient of many awards and honors. Dr. Chen's research interests include wireless communications and wireless networks, cognitive and nano-communications & computing.