Design and Analysis of the Key Management Mechanism in Evolved Multimedia Broadcast/Multicast Service

Yi Ren, *Member, IEEE*, Jyh-Cheng Chen, *Fellow, IEEE*, Jui-Chih Chin, and Yu-Chee Tseng, *Fellow, IEEE*

***Abstract*— 3GPP introduced the key management mechanism (KMM) in evolved multimedia broadcast/multicast service (eMBMS) to provide forward security and backward security for multicast contents. In this paper, we point out that KMM may lead to frequent rekeying and re-authentication issues due to eMBMS's characteristics: 1) massive group members; 2) dynamic group topology; and 3) unexpected wireless disconnections. Such issues expose extra load for both user equipment (UE) terminals and mobile operators. It seems prolonging the rekeying interval is an intuitive solution to minimizing the impact of the issues. However, a long rekeying interval is not considered the best operational solution due to revenue loss of content providers. This paper quantifies the tradeoff between the load of the UEs and the operators as well as the revenue loss of the content providers. Moreover, we emphasize how essential this rekeying interval has impacts on the problems. Using our proposed tradeoff model, the operators can specify a suitable rekeying interval to best balance the interest between the above three parties. The tradeoff model is validated by extensive simulations and is demonstrated to be an effective approach for the tradeoff analysis and optimization on eMBMS.**

***Index Terms*— Performance analysis, LTE, multimedia broadcast and multicast service (MBMS), key management.**

I. Introduction

In Long-Term Evolution (LTE), the 3rd Generation Partnership Project (3GPP) introduced the evolved Multimedia Broadcast/Multicast Service (eMBMS) [1]–[5] to multicast/broadcast multimedia content to *a large number* of User Equipment (UE) terminals. It is expected that eMBMS could significantly reduce delivery cost and increase efficiency. An example is live sports, where a large amount of users want to watch a game simultaneously. On January 27, 2014, the South Korean operator KT announced the world's first commercial LTE eMBMS services, named *Olleh LTE Play*.

As commercial eMBMS services are announced, both operators and content providers want to gain additional revenues by offering eMBMS services. A key issue is to guarantee that only users who have paid can enjoy the eMBMS service. 3GPP introduced Key Management Mechanism (KMM) [6] to provide forward security and backward security for multicast content, while a multicast group is maintained, in which only UEs belonging to the same group can receive the multicast data [7]. A group key is shared by the group members to encrypt and decrypt data. When a member joins/leaves the group, the group key needs to be updated to add/revoke the member, which is referred to as *rekeying*. Accordingly, the users holding *old keys* are unable to access subsequent contents. Such rekeying operations minimize security risks and provide both forward security and backward security.

The KMM, however, may lead to (1) frequent rekeying issue and (2) re-authentication issue due to eMBMS's characteristics: massive group members, dynamic group topology, and unexpected wireless disconnections. The frequent rekeying issue imposes signaling load for UEs when UEs join/leave the service group randomly. Considering Super Bowl using eMBMS for live show as an example, there are large number of users in the eMBMS service group, which may join the group to watch the show, or leave the group randomly (e.g., during quarter/half time breaks, or even caused by operators' resource allocation scheme [8]). Although such random behavior is not unique in eMBMS, it becomes more serious than that in other wireless multicast, such as ad hoc networks, sensor networks, and wireless local area networks. To be more specific, the number of UEs in an eMBMS multicast group is usually more than that in other wireless networks. An eMBMS service is likely to have ten thousand, or even more number of UEs in its multicast group. Given the large number of UEs in the group, such random behavior may cause much higher UE arrival (departure) rate than other wireless networks. A wireless sensor network, for example, targeted at environmental monitoring applications may have thousands of sensors. But these sensor nodes usually provide services throughout their whole lifetime without moving until their energy is depleted.

Manuscript received November 25, 2015; revised July 27, 2016; accepted September 22, 2016. Date of publication October 6, 2016; date of current version December 8, 2016. This work was supported by the Ministry of Science and Technology of Taiwan under Grant MOST 103-2221-E-009-110-MY3 and Grant MOST 105-2218-E-009-008. The work of Y. Ren was supported by MOST under Grant MOST 105-2221-E-009-101-MY3, Grant MOST 104-2221-E-009-100-MY3, Grant MOST 104-3115-E-009-006, and Grant MOST 104-3115-E-009-002. The work of Y.-C. Tseng was supported in part by MoE ATU Plan, in part by MOST under Grant MOST 104-2221-E-009-113-MY3, Grant MOST 105-2221-E-009-100-MY3, and Grant MOST 105-2218-E-009-003, in part by Academia Sinica under Grant AS-102-TP-A06, in part by ITRI, and in part by Delta. The associate editor coordinating the review of this paper and approving it for publication was K. Zeng.

The authors are with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan (e-mail: renyi@cs.nctu.edu.tw; jcc@cs.nctu.edu.tw; jcchin@cs.nctu.edu.tw; yctseng@cs.nctu.edu.tw).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

The re-authentication issue results in extra authentication load for Core Network (CN) and is mainly caused by missing rekeying information when UEs suffer from unexpected disconnections. Given the fact that a UE with old keys is unable to access subsequent eMBMS contents, the UE needs to perform authentication procedure with CN again to retrieve new keys. Such problem is more serious in eMBMS than in the aforementioned wireless networks. First, frequent rekeying increases the probability that rekeying information is lost. If there is no connection (e.g., blind spot, poor signal, or being out of coverage, etc.), the UE may miss the rekeying information. Second, in unicast, if the UE losses the rekeying information, retransmission mechanisms can be used. In eMBMS, however, the CN will still update the group key even if some of the UEs do not receive the rekeying information correctly. Therefore, those UEs which missed the rekeying information will not be able to derive new keys. Re-authentication procedure will be triggered, imposing extra authentication load for CN.

Overall, with short-term security keys, it will cause the above two issues. Alternatively, it seems that a very long-term key is a straightforward solution to minimize the impact for CN and UEs. However, how to prolong rekeying interval is not intuitive because long-term keys may compromise forward security and lead to revenue loss for content providers. That is, the UEs left the eMBMS service group can still access the subsequent contents because their keys are still under using. On the other hand, frequent rekeying imposes extra authentication load for CN and signaling load for UEs. The tradeoff is called the *security-performance tradeoff*.

The key question network operators might have is how to specify a rekeying interval to best balance the security-performance tradeoff. The answer to this question, however, may not exist due to the fact that such an interval should be determined by a network operator. Besides, management policies should also be taken into consideration. In this paper, we develop an analytical model to quantify the tradeoff between the load of the UEs and the operators (CN) as well as revenue loss of the content providers. As a first step toward this model, we firstly identify the frequent rekeying issue and re-authentication issue, and then define two performance metrics respectively to evaluate the load for UEs and CN. Next, targeting at an acceptable upper bound of revenue loss for a content provider, we model it as a performance metric to represent the interest of the content provider. After modeling the three metrics, we conduct extensive simulations using ns-2. The simulation results not only validate our analytical model but also show the impacts on UEs, CN, and content providers if the operator adjusts rekeying interval to alleviate the load for UEs and CN.

The rest of the paper is organized as follows. Section II presents background and problem statement. Section III presents the proposed algorithm. The analytical model is illustrated in Section IV, followed by the numerical results in Section V. In Section VI, we discuss optimal strategies. Section VII reviews the related work. In Section VIII, we conclude this paper.

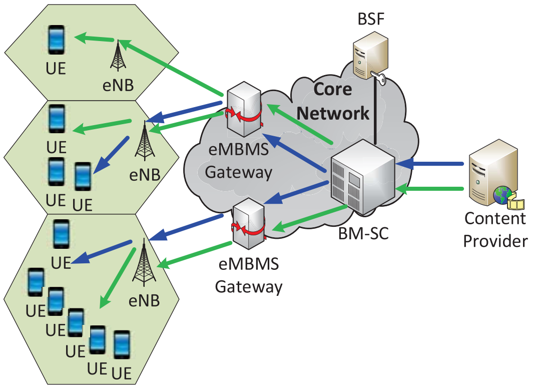


Fig. 1. Simplified example of eMBMS architecture.

II. Background and Problem Statement

In this section, we first introduce the background of eMBMS KMM, and then point out its shortcomings in practical applications.

A. Background

The eMBMS KMM architecture defined in [6] consists of Bootstrapping Server Function (BSF), Broadcast Multicast Service Centre (BM-SC), content provider, eMBMS gateway, and UEs, as shown in Fig. 1. More precisely, BSF is a part of Generic Bootstrapping Architecture (GBA) which establishes shared secrets between UEs and BM-SC. The BM-SC acts as an entry point for content delivery services (both live streams from encoders and multimedia contents from the content provider), and forwards the broadcast multicast packets to the eMBMS gateway from where the packets are distributed to evolved NodeB (eNB) in the Radio Access Network (RAN). In this paper, we only show BSF, BM-SC, and eMBMS gateway in the CN. Other components which are not relevant to this paper are not shown.

In order to protect the eMBMS data, 3GPP defined a set of four security keys in eMBMS KMM [2], [6], which are MBMS Request Key (MRK), MBMS Service Key (MSK), MBMS Traffic Key (MTK), and MBMS User Key (MUK). MRK and MUK are derived using GBA key derivation function [9]. MRK is to authenticate a UE to a BM-SC when performing key requests. MUK is used to protect the distribution of MSK, while MSK is used to protect a certain eMBMS session and the transmission of MTK. MTK is responsible for encrypting and decrypting eMBMS traffic. In short, MUK, MSK, and MTK are used to protect data (see their relationship in Fig. 2).

During an eMBMS service, MSK/MTK is (are) updated (referred to rekeying in this paper) when one of the following events happens: a) Event 1 (**E1**): a new UE joins the eMBMS session; b) Event 2 (**E2**): a joined UE leaves the eMBMS session; c) Event 3 (**E3**): the timer of MSK expires; and d) Event 4 (**E4**): the timer of MTK expires. In order to update MSK/MTK, User Service Join procedure (for **E1**), User Service Leave procedure (for **E2**), MSK Periodic Update procedure (for **E3**), and MTK Periodic Update procedure (for **E4**) are conducted [2], [6], [10].

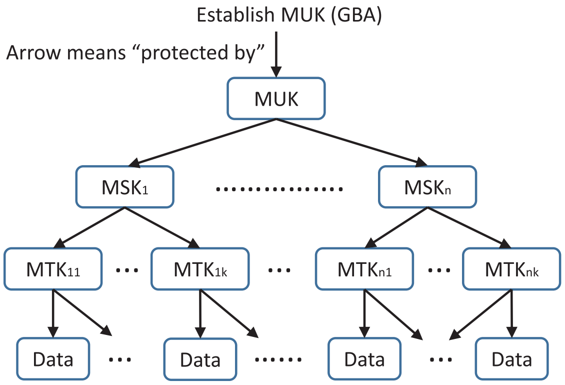


Fig. 2. Relationship between MUK, MSK, MTK, and eMBMS data.

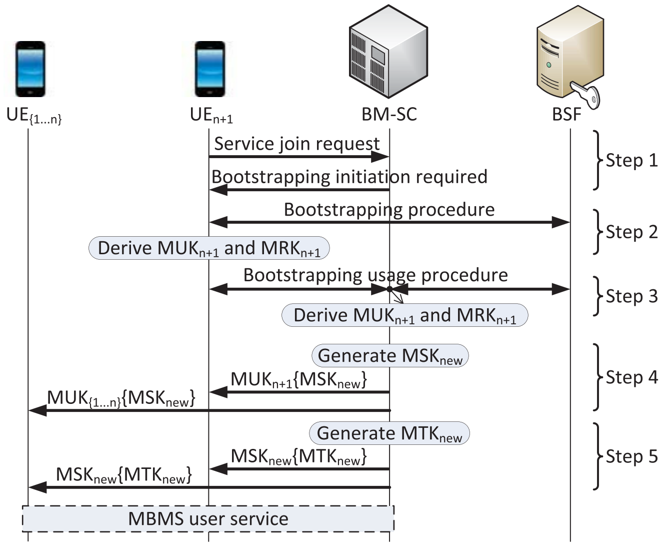


Fig. 3. Procedure of a new UE joins a MBMS user service - message flow.

Here, we show a simplified example of User Service Join procedure for **E1** in Fig. 3, where $\mathrm{UE}_{\{1 \dots n\}}$ denote the UEs which have already joined the service, and UE_{n+1} is a new UE.

- Step 1: The new UE, UE_{n+1}, first sends a service join request to the BM-SC. The BM-SC then will ask UE_{n+1} to initiate the bootstrap authentication procedure with the BSF.
- Step 2: The UE_{n+1} performs the bootstrapping authentication procedure with the BSF to obtain MRK_{n+1} and then derives MUK_{n+1} based on the MRK_{n+1}.
- Step 3: After the UE_{n+1} has derived MRK_{n+1} and MUK_{n+1}, it performs authentication with the BM-SC using the MRK_{n+1}.
- Step 4: The BM-SC generates a new MSK, $\mathrm{MSK}_{\mathrm{new}}$, and *unicasts MIKEY message [11] over UDP* to transport the $\mathrm{MSK}_{\mathrm{new}}$ to every UE that has joined the service by Dedicated Control Channel (DCCH) and Dedicated Traffic Channel (DTCH) [5], [6]. The message sent to UE_k ($k \in [1, n]$) is protected by the corresponding MUK_k.
- Step 5: The BM-SC generates a new MTK, $\mathrm{MTK}_{\mathrm{new}}$, encrypted by $\mathrm{MSK}_{\mathrm{new}}$, and multicasts it over UDP to every UE that has joined the service by MBMS point-to-multipoint Control Channel (MCCH) and MBMS point-to-multipoint Traffic Channel (MTCH) [5], [6].

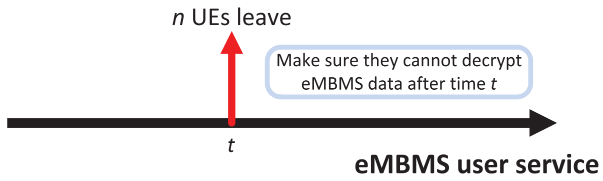


Fig. 4. An example of forward security.

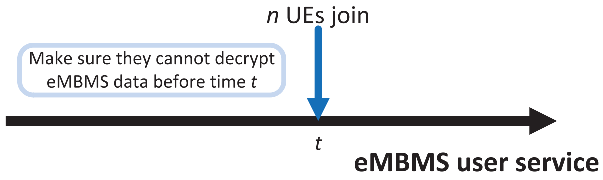


Fig. 5. Example of backward security.

B. Problem Statement

eMBMS KMM may lead to frequent rekeying issue and re-authentication issue. For the sake of security, KMM has to guarantee both forward security and backward security. In other words, a UE revoked from the eMBMS service group at time t will not be able to access the encrypted content after time t (see Fig. 4 as an example). In contrast, ensuring backward security requires that a UE, which joined the eMBMS service at time t, is not able to access any keys used to encrypt data before time t, as shown in Fig. 5. Formal definition of forward security and backward security are given in Definitions 1 and 2.

Definition 1 (Forward Security): Forward security is provided if for any set $R_t \subset \mathbb{UE}$, where R_t is a set of revoked UEs before time t. It is computationally infeasible for UEs from R_t working together to get any information about $\mathcal{K}_{t'}$ ($t' \geq t$), even when previous security keys $\{\mathcal{K}_1, \cdots, \mathcal{K}_{t-1}\}$ are available.

Definition 2 (Backward Security): Backward security is provided if for any set $\mathcal{A}_t \subset \mathbb{UE}$, where $\mathcal{A}_t$ is a set of added UEs after time t. It is computationally infeasible for UEs from $\mathcal{A}_t$ working together to obtain any knowledge about $\mathcal{K}_{t'}$ ($t' < t$), even when a set of security keys $\{\mathcal{K}_t, \mathcal{K}_{t+1}, \cdots, \mathcal{K}_n\}$ after time t are available.

Issue 1 (Frequent Rekeying Issue): By providing both forward security and backward security, we can minimize the security risk as well as protect content providers' interest from freeloaders. However, it will lead to the frequent rekeying issue if UEs join/leave the service frequently. More specifically, to guarantee forward security, if a joined UE leaves the eMBMS service (**E2**), the rest of the UEs need to update their MSK and MTK. After the UE left the service group, *rekeying* procedure is performed to update new keys $\mathrm{MTK}_{\mathrm{new}}$ and $\mathrm{MSK}_{\mathrm{new}}$ to the rest of UEs. The UE holding $\mathrm{MTK}_{\mathrm{old}}$ and $\mathrm{MSK}_{\mathrm{old}}$ will not be able to access the subsequent content, i.e., $\mathrm{MTK}_{\mathrm{old}}$ and $\mathrm{MSK}_{\mathrm{old}}$ are revoked. On the other hand, to ensure backward security, all UEs in the service have to update their MSK and MTK if a new UE joins the eMBMS service (**E1**) (see Step 4 and Step 5). In other words, rekeying rate grows when UE joining/leaving rate increases. As discussed in Section I, the characteristics of eMBMS lead to much higher UE joining/leaving rate than that in other wireless multicast cases, resulting in much higher rekeying rate as well.

Issue 2 (Re-authentication issue): Missing rekeying information will cause the re-authentication issue, and the above frequent rekeying issue makes it even more serious. Specifically, in KMM, security key(s) (we use $\mathcal{K}$ to denote either MSK or MTK, etc.) is/are updated to provide forward security. In other words, the security key $\mathcal{K}_i$ is evolved if and only if one knows the previous key, i.e., $\mathcal{K}_i \Rightarrow \mathcal{K}_{i+1}$ and $\mathcal{K}_i \not\Rightarrow \mathcal{K}_j$ $(i \geq 1, j \geq i+2)$. The key evolvement (say from $\mathcal{K}_i$ to $\mathcal{K}_j$) will fail if any key $\mathcal{K}_k$ $(i < k < j)$ is missing. In eMBMS, the consequence of key evolvement failure is that the UE will not be able to decrypt the eMBMS content encrypted by the new key $\mathcal{K}_j$. The eMBMS service is thus interrupted from UE's perspective.

To be more specific, the rekeying information may be lost in the following two cases: (1) MSK_{new} may be lost due to UDP transmission. The updated MSK_{new} is unicast in MIKEY message to every UE joined the eMBMS services over UDP [5], [6]. There is no ACK to confirm that the UEs have received the updated MSK_{new} correctly [6]. (2) MTK_{new} may also be lost during *multicast* transmission. In Step 5 in Fig. 3, the MTK_{new} is multicast to every UE joined the service over UDP [5], [6]. A UE will not send an error message to the BM-SC because of not receiving an MTK message [6]. The eMBMS KMM will still update security keys even if some UEs do not receive the rekeying information correctly.

In short, missing MTK_{new} will cause that the UEs cannot decrypt current eMBMS content. In addition, missing MSK_{new} will lead to that the UEs cannot obtain MTK_{new} encrypted by the MSK_{new} (see Step 5 in Fig. 3). Therefore, a UE will not be able to continue to access eMBMS content if any of these keys is missing. Thus, the UE needs to perform authentication procedure with the BM-SC again to retrieve new keys, which leads to the re-authentication issue.

III. Proposed Dynamic Rekeying Algorithm (DRA)

To solve the aforementioned issues, we propose an algorithm called Dynamic Rekeying Algorithm (DRA). The DRA is performed by operators to determine whether rekeying should be conducted. No modification is required at the UE side. DRA is designed to update security key(s) based on a dynamic time slot, instead of updating them whenever a UE joins/leaves the eMBMS session (**E1/E2** happens). It is easy to know that a very long rekeying time slot can alleviate the frequent rekeying and re-authentication issues. However, it may incur free enjoying time for freeloaders, which leads to revenue loss of content providers. To balance the tradeoff, we define a performance metric as an upper bound of acceptable revenue loss for the interest of the content providers. Rekeying is then performed based on the upper bound of revenue loss.

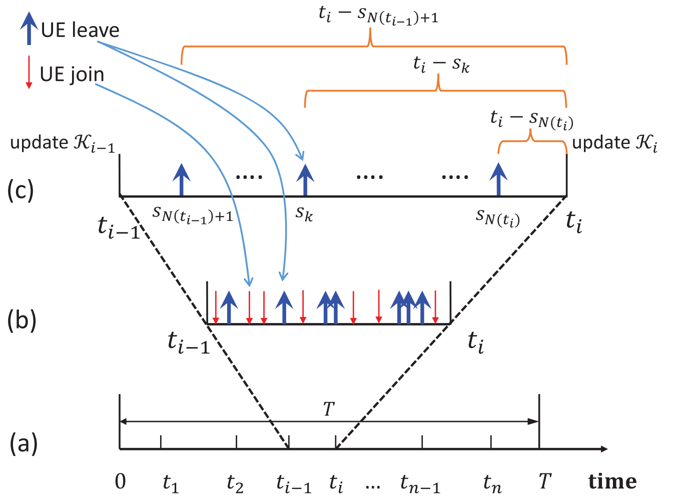


Fig. 6. An example of possible free enjoy time when UEs leave the eMBMS session.

To be more specific, Fig. 6 shows the dynamic key update procedure of DRA. For simplicity, we use $\mathcal{K}$ to denote either MSK or MTK, and *Update-Key* to present MSK/MTK updating procedures. Once *Update-Key* is triggered, the security key, $\mathcal{K}_i$, is updated to a new key, $\mathcal{K}_{i+1}$, i.e., $\mathcal{K}_i \rightarrow \mathcal{K}_{i+1}$. In Fig. 6(a) we can see that *Update-Key* is triggered by dynamic time slots. At time $\{t_1, t_2, \cdots, t_i, \cdots, t_n\}$, the security key, $\mathcal{K}$, is updated as time goes by, i.e., $\mathcal{K}_1 \rightarrow \mathcal{K}_2 \rightarrow \cdots \rightarrow \mathcal{K}_i \rightarrow \cdots \rightarrow \mathcal{K}_n$. Fig. 6(b) further illustrates a zoom-in picture of the time slot $[t_{i-1}, t_i]$. The red arrow (with smaller arrow size) denotes a UE joining the eMBMS service, and the blue one (with bigger arrow size) denotes a UE leaving the service. We can see that even more than one (could be many) UEs join/leave the service during $[t_{i-1}, t_i]$, the DRA only performs *Update-Key* two times at t_{i-1} and t_i, respectively. Such design significantly reduces the rekeying cost and frequency for both UEs and CN. However, left UEs are still able to access the subsequence content by t_i because their security key $\mathcal{K}_{i-1}$ is still under using, which leads to revenue loss of content providers.

Content providers' interest should be also taken into consideration. Normally, content providers charge for the eMBMS multimedia contents they provide. For example, quota-based plan allows users to select from different usage quota limits. Volume-based (usage-based) plan charges users based on their usage [12], [13]. For the *pay for what you use* pricing model,[1] one of the basic requirements is to record the volume used by the users. Missing the usage records leads to revenue loss for the content providers. Specifically, let us further zoom in the time slot $[t_{i-1}, t_i]$ and show it in Fig. 6(c). We can see that the key $\mathcal{K}_{i-1}$ obtained at t_{i-1} is valid for the whole time slot $[t_{i-1}, t_i)$. Considering a UE leaves the group at s_k as an example, the UE can still freely enjoy the multicast content during $[s_k, t_i)$ because it holds $\mathcal{K}_{i-1}$ (forward security is not guaranteed, see Definition 1).

[1] Unlimited, flat-rate plan for multimedia contents is out of the scope of this paper.

In contrast, if a UE joins the group at s_k, the UE is able to decrypt the multicast content transmitted during $[t_{i-1}, s_k]$ (backward security is not provided, see Definition 2). The two cases show that prolonging rekeying time interval leads to revenue loss (free enjoy time) for content providers. Therefore, selecting a suitable rekeying time interval is a tradeoff between UE (signaling cost), operators (CN cost and RAN cost), and content providers (revenue loss).

Here, we quantify the free enjoy time that the content provider is going to lose if the rekeying intervals are prolonged. An accumulated free enjoy time factor constrained by both forward security and backward security is defined as follows:

$$\phi = \omega_b \sum_{k=N(t_{i-1})+1}^{N(t_i)} \Big(s_k - t_{i-1}\Big) + \omega_f \sum_{k=N(t_{i-1})+1}^{N(t_i)} \Big(t_i - s_k\Big), \tag{1}$$

for the upper bound of the free enjoy time, where ω_b and ω_f are weights for backward security and forward security, $N(t_i)$ is the number of UEs leaving the multicast group within [0, t_i], and $s_{N(t_i)}$ is the time when $N(t_i)$-th UE leaves the group. By adjusting ω_b and ω_f, operators can easily increase or decrease the weight of either backward security or forward security based on their management policies.

In eMBMS, we consider that forward security is more important than backward security. Normally it is less motivated for UEs to compromise backward security because they have to record the multicast content in advance and then decrypt them using the key $\mathcal{K}_{i-1}$ obtained at s_k to get a small piece of free multicast content, e.g., multicast content transmitted in $[t_{i-1}, s_k)$. For simplicity, we set $\omega_b = 0$ and $\omega_f = 1$ in Eq. (1) to get the accumulated free enjoy time factor constrained by forward security,[2]

$$\phi = \sum_{k=N(t_{i-1})+1}^{N(t_i)} \Big(t_i - s_k\Big), \tag{2}$$

for the upper bound free enjoy time. Here, we refer the excess time interval $[s_k, t_i)$ as free enjoy time interval. When the accumulated free enjoy time interval, ϕ, reaches to a predefined threshold, ϕ_{th}, the *Update-Key* is triggered for rekeying procedure. Operators thus can easily adjust rekey time interval by setting ϕ_{th}, while the interests of UEs, operators, and content providers are taken into consideration.

Discussion: Mobile operators could interpret ϕ in two ways once ϕ is derived: revenue gain and revenue loss. When ϕ is considered as revenue gain, Eq. (2) quantifies extra incomes for content providers. For example, nowadays mobile operators usually charge a certain rate for a certain time. If a mobile operator will charge \$0.1 for 10 seconds, a user will still need to pay for \$0.1 even if the user only talks for 3 seconds. Similarly, the ϕ can be considered as the extra gain of content providers if mobile operators ask users to pay for the whole rekeying time slot.

Whereas, when ϕ is considered as the revenue loss of content providers, there could be freeloader attacks against such setting. Specifically, attackers could try to register for a very short time and only pay for the actual registered time, and then enjoy the rest of the rekeying time slots for free. For example, the attacker registers and pays for only 5 seconds in the beginning of every slot. If the rekeying time slots are long (say 120 seconds), the attacker could pay less for the content. However, to enjoy the service continuously, the attacker needs to jump in/out the service frequently. Although there could be more countermeasures for such attack, here we introduce three solutions.

1) Charge connection fee: Nowadays, many operators charge connection fee, say \$1.99, for the first 3 minutes, and then charge additional \$0.1 for each 10 seconds. A user will be charged at least for \$1.99 even if the user talks for less than 3 minutes. Similar idea could be used for eMBMS. For instance, mobile operators could charge κ rekeying time slots (say $\kappa = 3$) for connection fee when a UE joins the eMBMS service. In other words, a user has to pay for the first κ rekeying time slots no matter how long it stays in the service.
2) Block users with unusual registration frequencies: For UEs with unusual registration frequencies, mobile operators could block the UEs for a certain time interval, which can be exponentially increased. In addition, Turing test mechanism could be applied (e.g., CAPTCHAS [14]). Those users with unusual registration frequencies could be asked for some tests that are easy for humans to pass but difficult for computers to understand.
3) Change the length of rekeying time slot dynamically: The rekeying time slot can be changed dynamically so an attacker will not be able to figure out the length of rekeying slot.

As a conclusion, mobile operators can specify the rekeying time interval according to their management policies. Our study quantifies the accumulated free enjoy time (potential revenue gain/loss) and gives theoretical guidelines for operators to configure the parameters. The operators can interpret ϕ based on their needs.

IV. Performance Analysis

In this section, we propose an analytic model to investigate the rekeying cost and re-authentication cost of DRA where the rekeying interval is prolonged. For performance comparison, we denote the original rekeying based on UE join/leave as Traditional Rekeying Algorithm (TRA).

The parameters used in the analysis are listed in Table I. In the analysis, the inter-arrival time of the UEs is assumed to be exponentially distributed with mean $1/\lambda$. When a UE joins the eMBMS session, the UE stays in the session for a time interval, t_u, with the expected value $\frac{1}{\theta}$, probability density function (pdf) $f_u(\cdot)$, cumulative distribution function (CDF) $F_u(\cdot)$, and the Laplace transform $f_u^*(s)$. Further, let N and M be the number of UEs joined the eMBMS session and the number of UEs left the eMBMS session within an observation time interval T_s. The problem can be modeled as an

[2] It can be modified to support backward security, or both backward security and forward security by adjusting ω_b and ω_f.

TABLE I

LIST OF PARAMETERS

	Parameter
UE resident time in an eMBMS session	t_u
pdf of t_u	f_u
CDF of t_u	F_u
Laplace transform of t_u	$f_u^*(s)$
The expected value of t_u	$\frac{1}{\theta}$
The expected UE arrival rate	λ
Observation time interval	T_s
The number of UE arrived during T_s	N
The number of UE left during T_s	M
The expected UE departure rate	λ_d
Accumulated free enjoy time	ϕ
UE unintended disconnection rate	ω
UE unintended disconnection time	t_d
The expected value of t_d	τ
pdf of t_d	$f_d(t_d)$
CDF of t_d	$F_d(t_d)$
Laplace transform of t_d	$f_d^*(s)$
Rekeying rate	λ_R
Time interval between two rekeying operations	t_R
pdf of t_R	$f_R(t_R)$
CDF of t_R	$F_R(t_R)$
The time interval the UE enters the disconnection status and when the first rekeying operation arrives	t_r
pdf of t_r	$f_r(t_r)$
Re-authentication probability	p
Re-authentication cost for CN	$\mathcal{N}$

$M/G/\infty$ system. In other words, observed by an eMBMS session, UE arrivals follow Poisson process and are served immediately. The time period that a UE stays in the session t_u follows a general distribution.

In Section IV-A, we analyze the rekeying cost of TRA and DRA. We then derive re-authentication costs of TRA and DRA in Section IV-B.

A. Rekeying Cost

1) Rekeying Cost of TRA: Recall that in TRA whenever a UE joins/leaves the eMBMS session, *Update-Key* is triggered to assign new keys to add/revoke UEs to/from the eMBMS multicast group. It is straightforward to know that the expected total rekeying cost is the total number of UEs joined the group and left the group, i.e., $E[N] + E[M]$, where $E[N]$ is the expected number of N, and $E[M]$ is the expected number of M. In an observation time interval, T_s, $E[N]$ is computed as:

$$E[N] = \lambda T_s. \tag{3}$$

Similarly, $E[M]$ in T_s is:

$$E[M] = \lambda_d T_s, \tag{4}$$

where λ_d is the mean of UE's departure rate in T_s.

Next, we will derive the relationship between UE arrival rate, λ, and UE departure rate, λ_d. We first consider the probability that a UE *arriving at time s* will leave by time t is $P\{t_u \leq t-s\}$, i.e., $F_u(t-s)$. Then, $P\{t_u > t-s\} = 1-F_u(t-s)$ is the probability that a UE arriving at time s will still be present at time t. Therefore, the probability that an arbitrary UE arrived before t is still in the session at t is given by: $P_t = \int_0^t P\{t_u > t-s|S=s\}P\{S=s\}ds$. Because arrivals of UEs follow Poisson distribution, according to Theorem 5.2 in [15], $P\{S = s\}$ is uniform distributed on $(0,t)$. Thus, $P\{S=s\} = \frac{1}{t}$. We have:

$$\begin{aligned} P_t &= \frac{1}{t}\int_0^t P\{t_u > t-s|S=s\}ds \\ &= \frac{1}{t}\int_0^t \Big[1 - F_u(t-s)\Big]ds = \frac{1}{t}\int_0^t \Big[1-F_u(s)\Big]ds. \end{aligned}$$

From [16], the probability that m numbers of UEs leave the session at time t is given by:

$$P\{M(t) = m\} = \frac{\Big[\lambda(1-P_t)t\Big]^m e^{-\lambda(1-P_t)t}}{m!}. \tag{5}$$

From Eq. (5), we can derive the departure rate of UEs in the session as:

$$\begin{aligned} \lambda_d &= \lambda(1-P_t) \\ &= \lambda\Big\{1 - \frac{1}{t}\int_0^t \Big[1-F_u(s)\Big]ds\Big\}. \end{aligned} \tag{6}$$

We observe from Eq. (6) that λ_d is a random variable over t. Initially, λ_d is zero because no UE leaves the session at the beginning. As $t \rightarrow \infty$, we see that P_t goes to zero. It means that the inter-departure process is Poisson process in steady state, which is precisely the same as the arrival process. In other words, in steady state, the departure rate of UEs, λ_d, is exactly the same as the arrival rate, λ, i.e., $\lambda_d = \lambda$. Thus, Eq. (4) is rewritten as:

$$E[M] = \lambda_d T_s = \lambda T_s. \tag{7}$$

From Eq. (3) and Eq. (7), the rekeying cost of TRA in T_s is given as:

$$C_{TRA} = E[N] + E[M] = 2\lambda T_s. \tag{8}$$

2) Rekeying Cost of DRA: Recall that the basic idea of DRA is to update security keys when the accumulated free enjoy time ϕ increases to the predefined threshold ϕ_{th} no matter how many UEs join/leave the session. That is, the keys are changed based on time slots, $\Delta t_i, i \in [1,n]$, constrained on ϕ_{th}. The rekeying cost of DRA is then derived as:

$$C_{DRA} = \frac{T_s}{E(\Delta t_i)}. \tag{9}$$

In the following, we will derive $E(\Delta t_i)$ in Eq. (9). As illustrated in Fig. 6, UEs depart at time $s_{N(t_{i-1})+1}, s_{N(t_{i-1})+2}, \cdots, s_{N(t_i)}$. The expected sum of free enjoy times of UEs depart in (t_{i-1}, t_i) is given by:

$$\begin{aligned} E[\phi] &= E\Big[\sum_{k=N(t_{i-1})+1}^{N(t_i)} (t_i - s_k)\Big] \\ &= E\Big[E\Big[\sum_{k=N(t_{i-1})+1}^{N(t_i)} (t_i - s_k)\Big| N(t_i), N(t_{i-1})\Big]\Big] \\ &\triangleq E[\mathbb{A}], \end{aligned} \tag{10}$$

where $\mathbb{A} = E\Big[\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Big|N(t_i), N(t_{i-1})\Big]$. We then get a conditional $\mathbb{A}$ for $N(t_i) = \mathfrak{n}_2$, and $N(t_{i-1}) = \mathfrak{n}_1$ as:

$$
\begin{aligned}
E\Bigg[&\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Bigg|N(t_i) = \mathfrak{n}_2, N(t_{i-1}) = \mathfrak{n}_1\Bigg] \\
&= E\Bigg[\sum_{k=\mathfrak{n}_1+1}^{\mathfrak{n}_2}(t_i - s_k)\Bigg|N(t_i) = \mathfrak{n}_2, N(t_{i-1}) = \mathfrak{n}_1\Bigg] \\
&= E\Bigg[\sum_{k=\mathfrak{n}_1+1}^{\mathfrak{n}_2}(t_i - s_k)\Bigg] \\
&= E\Bigg[(\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i) - \sum_{k=\mathfrak{n}_1+1}^{\mathfrak{n}_2}(s_k)\Bigg] \\
&= (\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i) - E\Bigg[\sum_{k=\mathfrak{n}_1+1}^{\mathfrak{n}_2} s_k\Bigg]. \qquad (11)
\end{aligned}
$$

In steady state, the output of $M/G/\infty$ is Poisson process. From [15, Th. 5.2], the $N(t_i) - N(t_{i-1})$ departure times $s_{N(t_{i-1})+1}, s_{N(t_{i-1})+2}, \cdots, s_{N(t_i)}$ have the same distribution as the order statistics corresponding to $\mathfrak{n}$ independent random variables uniformly distributed on the interval (t_{i-1}, t_i). We then have:

$$
E\Bigg[\sum_{k=\mathfrak{n}_1+1}^{\mathfrak{n}_2} s_k\Bigg] = \frac{1}{2}(\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i + t_{i-1}). \qquad (12)
$$

According to Eq. (12), Eq. (11) is then rewritten as:

$$
\begin{aligned}
E\Bigg[&\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Bigg|N(t_i) = \mathfrak{n}_2, N(t_{i-1}) = \mathfrak{n}_1\Bigg] \\
&= (\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i) - \frac{1}{2}(\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i + t_{i-1}) \\
&= \frac{1}{2}(\mathfrak{n}_2 - \mathfrak{n}_1)E(t_i - t_{i-1}),
\end{aligned}
$$

which yields:

$$
\begin{aligned}
\mathbb{A} &= E\Bigg[\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Bigg|N(t_i), N(t_{i-1})\Bigg] \\
&= \frac{1}{2}\Big[N(t_i) - N(t_{i-1})\Big]E(t_i - t_{i-1}) \\
&= \frac{1}{2}\Big[N(t_i) - N(t_{i-1})\Big]E(\Delta t_i)
\end{aligned}
$$

and thus, Eq. (10) is rewritten as:

$$
\begin{aligned}
E\Bigg[&\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Bigg] \\
&= E\Bigg[\frac{1}{2}\Big[N(t_i) - N(t_{i-1})\Big]E(\Delta t_i)\Bigg] \\
&= \frac{E(\Delta t_i)}{2}E\Big[N(t_i) - N(t_{i-1})\Big] \\
&= \frac{E(\Delta t_i)}{2}\lambda_d E(\Delta t_i) \\
&= \frac{E(\Delta t_i)^2}{2}\lambda_d. \qquad (13)
\end{aligned}
$$

As discussed above, in steady state, the UE departure rate is exactly the same as the UE arrival rate, i.e., $\lambda_d = \lambda$.

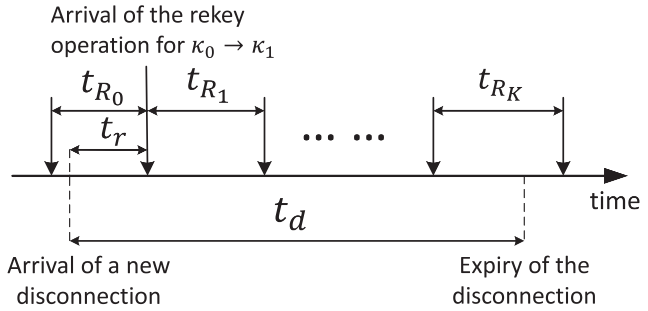

Arrival of the rekey operation for $\kappa_0 \to \kappa_1$
t_{R_0}
t_{R_1}
t_{R_K}
t_r
$\cdots\ \cdots$
time
t_d
Arrival of a new disconnection
Expiry of the disconnection

Fig. 7. Rekeying and disconnection timing diagram.

Eq. (13) is then rewritten as:

$$
E\Bigg[\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\Bigg] = \frac{E(\Delta t_i)^2}{2}\lambda.
$$

It is easy to know that $\phi_{th} = E\big[\sum_{k=N(t_{i-1})+1}^{N(t_i)}(t_i - s_k)\big]$, which yields:

$$
E(\Delta t_i) = \sqrt{\frac{2\phi_{th}}{\lambda}}, \qquad (14)
$$

and hence Eq. (9) is rewritten as:

$$
C_{DRA} = T_s\sqrt{\frac{\lambda}{2\phi_{th}}}. \qquad (15)
$$

B. Ue Re-Authentication Probability and Re-Authentication Cost for CN

Let ω, τ, and λ_R denote the disconnection rate of a UE in the eMBMS session, the mean value of its disconnection time, and the rekeying rate in the eMBMS session, respectively. The disconnection arrivals follow Poisson process with rate ω. The disconnection time, t_d, as shown in Fig. 7, is independent and identically distributed (i.i.d.) random variables with CDF $F_d(t_d)$, pdf $f_d(t_d)$, and the Laplace-Stieltjes Transform: $f_d^*(s) = \int_{t=0}^{\infty} e^{-st} f_d(t)dt$.

Moreover, as shown in Fig. 7, $t_{R_0}, t_{R_1}, \cdots, t_{R_K}$ denote the time intervals between rekeying operations in the eMBMS session with pdf $f_R(t_{R_K})$ and CDF $F_R(t_{R_K})$. Let t_r denote the interval between the UE enters the disconnection period and the time when the first rekeying operation arrives. Furthermore, let p denote the re-authentication probability when a UE is in disconnection period. In other words, the probability that at least one rekeying operation happens in the disconnection period of the UE is also p. Therefore,

$$
p = P\{t_d > t_r\} = 1 - P\{t_d \le t_r\}. \qquad (16)
$$

The probability that no rekeying operation happens in t_d is:

$$
\begin{aligned}
P\{t_d \le t_r\} &= \int_{t=0}^{\infty} P\{t_d \le t_r | t_r = t\} f_r(t)dt \\
&= \int_{t=0}^{\infty} P\{t_d \le t | t_r = t\} f_r(t)dt \\
&= \int_{t=0}^{\infty} P\{t_d \le t\} f_r(t)dt \\
&= \int_{t=0}^{\infty} F_d(t) f_r(t)dt \\
&= \int_{t=0}^{\infty}\int_{t_d=0}^{t} f_d(t_d) f_r(t)dt_d dt, \qquad (17)
\end{aligned}
$$

where $f_r(t)$ is the pdf of t_r. According to the *Excess Life Theorem* in [15],

$$f_r(t) = \lambda_R \int_{s=t}^{\infty} f_R(s)ds \\ = \lambda_R \Big[1 - F_R(t)\Big]. \quad (18)$$

Considering a time interval t_u while a UE stays in the eMBMS session, there are ωt_u disconnections happened totally. The expected value of total disconnections is $\omega E[t_u] = \omega \frac{1}{\theta}$. An UE then needs to re-authenticate $\omega \frac{1}{\theta} p$ times in average in those $\omega \frac{1}{\theta}$ disconnections. The expected value of total UE arrivals in the observation time interval T_s is λT_s. The total re-authentication cost for the CN, $\mathcal{N}$, then can be expressed as:

$$\mathcal{N} = \Big(\omega \frac{1}{\theta} p\Big)\Big(\lambda T_s\Big) = \frac{\omega \lambda T_s}{\theta} p. \quad (19)$$

1) UE Re-Authentication Probability and Re-Authentication Cost of TRA: In steady state, the output of M/G/∞ follows Poisson process in which UE departure rate is exactly the same as the UE arrival rate. In TRA, whenever a UE joins/leaves the eMBMS session, rekeying operation is triggered. Therefore, the rekeying operation is a Poisson process with rate $\lambda_R = 2\lambda$. Hence, from Eq. (18), Eq. (17) is rewritten as:

$$\begin{aligned} & P\{t_d \le t_r\} \\ &= \int_{t=0}^{\infty} \int_{t_d=0}^{t} f_d(t_d) \lambda_R \Big[1 - F_R(t)\Big] dt_d dt \\ &= \int_{t=0}^{\infty} \int_{t_d=0}^{t} f_d(t_d) \lambda_R e^{-\lambda_R t} dt_d dt \\ &= \int_{t_d=0}^{\infty} \int_{t=t_d}^{\infty} f_d(t_d) \lambda_R e^{-\lambda_R t} dt dt_d \\ &= \int_{t_d=0}^{\infty} f_d(t_d) e^{-\lambda_R t_d} dt_d \\ &= f_d^*(\lambda_R) = f_d^*(2\lambda). \end{aligned}$$

Eq. (16) is then rewritten as:

$$p_{TRA} = 1 - f_d^*(2\lambda), \quad (20)$$

and Eq. (19) is given as:

$$\mathcal{N}_{TRA} = \frac{\omega \lambda T_s}{\theta} p_{TRA} = \frac{\omega \lambda T_s}{\theta} \Big[1 - f_d^*(2\lambda)\Big]. \quad (21)$$

Because the UE's unexpected disconnection time distribution, t_d, is assumed to be a general distribution, here we drive p_{TRA} and $\mathcal{N}_{TRA}$ based on four UE unexpected disconnection time distributions as follows.

a) Gamma distribution: If $f_d(t)$ is the pdf of the Gamma distribution with a shape parameter π and a scale parameter $\frac{\tau}{\pi}$, its Laplace transform $f_d^*(s)$ is given as $f_d^*(s) = (1 + \frac{\tau}{\pi} s)^{-\pi}$.

Hence, Eqs. (20) and (21) are rewritten as:

$$p_{TRA} = 1 - \Big(1 + \frac{2\lambda\tau}{\pi}\Big)^{-\pi},$$

and

$$\mathcal{N}_{TRA} = \frac{\omega \lambda T_s}{\theta} \Big[1 - \Big(1 + \frac{2\lambda\tau}{\pi}\Big)^{-\pi}\Big],$$

respectively.

We are especially interested in Gamma distribution. The reason is that the distribution of any positive random variable can be approximated by a combination of Gamma distribution as stated in [17, Lemma 3.9].

b) Hyper-Erlang distribution: It has been shown that hyper-Erlang distribution has very general approximation capability for the probability distribution of any positive random variable [17], [18]. Its Laplace transform $f_u^*(s)$ is given as: $f_u^*(s) = \sum_{j=1}^{J} \omega_j \left(\frac{\alpha_j \beta_j}{s + \alpha_j \beta_j}\right)^{\alpha_j}$ where $\omega_j \ge 0, \sum_{j=1}^{J} \omega_j = 1$, and J, α_1, α_2, $\cdots$, α_J are nonnegative integers. β_1, β_2, $\cdots$, β_J are positive numbers.

Hence, Eqs. (20) and (21) are rewritten as:

$$p_{TRA} = 1 - \sum_{j=1}^{J} \omega_j \Big(\frac{\alpha_j \beta_j}{2\lambda + \alpha_j \beta_j}\Big)^{\alpha_j},$$

and

$$\mathcal{N}_{TRA} = \frac{\omega \lambda}{\theta \mu} \Big[1 - \sum_{j=1}^{J} \omega_j \Big(\frac{\alpha_j \beta_j}{2\lambda + \alpha_j \beta_j}\Big)^{\alpha_j}\Big],$$

respectively.

The hyper-Erlang distribution can be used to approximate log-normal distribution which has been used for statistical fitting [19]. It is also suitable to approximate t_d that is either Sum of Hyper-Exponentials (SOHYP) or Coxian distributed or more generally phase-type distributed [16], [20], [21].

c) Erlang distribution: The Laplace transform of Erlang distribution, $Erlang(k, \frac{1}{\tau})$, is given as $f_u^*(s) = \left(\frac{1}{1+\tau s}\right)^k$. Hence, Eqs. (20) and (21) are rewritten as: $p_{TRA} = 1 - \left(\frac{1}{1+2\tau\lambda}\right)^k$, and $\mathcal{N}_{TRA} = \frac{\omega\lambda T_s}{\theta}\Big[1 - \left(\frac{1}{1+2\tau\lambda}\right)^k\Big]$, respectively.

d) Exponential distribution: This distribution is a special case of Gamma distribution. The Laplace transform of the time interval, t_d, with the distribution Exp($\frac{1}{\tau}$) is $f_u^*(s) = \frac{1}{1+\tau s}$.

Hence, Eqs. (20) and (21) are rewritten as: $p_{TRA} = 1 - \frac{1}{1+2\tau\lambda} = \frac{2\tau\lambda}{1+2\tau\lambda}$, and $\mathcal{N}_{TRA} = \frac{\omega\lambda T_s}{\theta}\Big[\frac{2\tau\lambda}{1+2\tau\lambda}\Big] = \frac{2\omega\tau\lambda^2 T_s}{\theta(1+2\tau\lambda)}$, respectively.

2) UE Re-Authentication Probability and Re-Authentication Cost of DRA: In DRA, from Eq. (14), we have obtained that the rekeying operation happens per $\sqrt{\frac{2\phi_{th}}{\lambda}}$. In other words, we can obtain rekeying rate $\lambda_R = \sqrt{\frac{\lambda}{2\phi_{th}}}$. The rekeying operation then has a pmf given by:

$$p(\mathfrak{m}) = \frac{1}{T_s}\sqrt{\frac{2\phi_{th}}{\lambda}}, \quad \mathfrak{m} \in \mathbb{N}^0, \mathfrak{m} \in \Bigg[0, \Bigg\lfloor T_s \sqrt{\frac{\lambda}{2\phi_{th}}} \Bigg\rfloor \Bigg).$$

Its CDF then is given as:

$$F_R(t) = \begin{cases} \frac{\mathfrak{m}}{T_s}\sqrt{\frac{2\phi_{th}}{\lambda}}, & \mathfrak{m}\sqrt{\frac{2\phi_{th}}{\lambda}} \le t < (\mathfrak{m}+1)\sqrt{\frac{2\phi_{th}}{\lambda}} \\ 1, & (\mathfrak{m}+1)\sqrt{\frac{2\phi_{th}}{\lambda}} \le t < T_s, \end{cases} \quad (22)$$

where $\mathfrak{m} \in \mathbb{N}^0, \mathfrak{m} \in \Big[0, \lfloor T_s \sqrt{\frac{\lambda}{2\phi_{th}}} \rfloor\Big)$. Hence, from Eqs. (18) and (22), Eq. (17) is rewritten as:

$$\begin{aligned} & P(t_d \le t_r) \\ &= \int_{t_r=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \int_{t_d=0}^{t_r} f_d(t_d) f_r(t_r) dt_d dt_r \end{aligned}$$

(since $t_r \leq$ rekey time interval)

$$= \int_{t_r=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \int_{t_d=0}^{t_r} f_d(t_d)\lambda_R\Big[1 - F_R(t_r)\Big]dt_d dt_r$$

$$= \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \int_{t_r=t_d}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} f_d(t_d)\lambda_R\Big[1 - F_R(t_r)\Big]dt_r dt_d$$

$$= \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \int_{t_r=t_d}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} f_d(t_d)\lambda_R dt_r dt_d$$

$$\Bigg(\text{from Eq. (22)}, \;\; F_R(t_r) = 0, \;\; \text{if } 0 \leq t_r < \sqrt{\frac{2\phi_{th}}{\lambda}}\Bigg)$$

$$= \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \lambda_R f_d(t_d)\Big(\sqrt{\frac{2\phi_{th}}{\lambda}} - t_d\Big)dt_d$$

$$= \lambda_R\sqrt{\frac{2\phi_{th}}{\lambda}} \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} f_d(t_d)dt_d - \lambda_R \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} f_d(t_d)t_d dt_d$$

$$= F_d(\sqrt{\frac{2\phi_{th}}{\lambda}}) - F_d(\sqrt{\frac{2\phi_{th}}{\lambda}}) + \lambda_R \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} F_d(t_d)dt_d$$

$$= \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} F_d(t_d)dt_d$$

Eq. (16) is then rewritten as:

$$p_{DRA} = 1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} F_d(t_d)dt_d \tag{23}$$

and Eq. (19) is given as:

$$\mathcal{N}_{DRA} = \frac{\omega\lambda T_s}{\theta}\Bigg[1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t_d=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} F_d(t_d)dt_d\Bigg]. \tag{24}$$

Again, we take Gamma distribution, hyper-Erlang distribution, Erlang distribution, and exponential distribution as examples for the distribution of t_d.

a) Gamma distribution: If $f_d(t; \pi, \frac{\tau}{\pi})$ is the pdf of the Gamma distribution with a shape parameter π and a scale parameter $\frac{\tau}{\pi}$, its CDF is given as $F(t; \pi, \frac{\tau}{\pi}) = \frac{\gamma(\pi, \frac{t\pi}{\tau})}{\Gamma(\pi)}$. Eqs. (23) and (24) are rewritten as:

$$p_{DRA} = 1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \frac{\gamma(\pi, \frac{t\pi}{\tau})}{\Gamma(\pi)}dt, \tag{25}$$

and

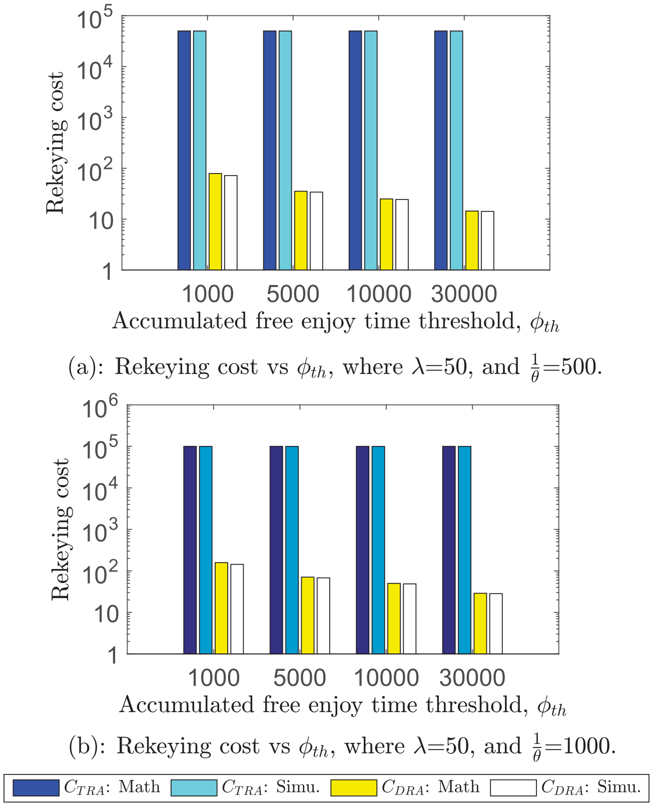
$$\mathcal{N}_{DRA} = \frac{\omega\lambda T_s}{\theta}\Bigg[1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \frac{\gamma(\pi, \frac{t\pi}{\tau})}{\Gamma(\pi)}dt\Bigg]. \tag{26}$$

b) Hyper-Erlang distribution: The hyper-Erlang distribution [18] has the following pdf:

$$f_d(t) = \sum_{j=1}^{J} \omega_j \frac{(\alpha_j\beta_j)^{\alpha_j} t^{\alpha_j - 1}}{(\alpha_j - 1)!} e^{-\alpha_j\beta_j t}, \quad t \geq 0. \tag{27}$$

Let $F_d(t)$ denote the CDF of a hyper-Erlang distribution given in Eq. (27). Let $\bar{F}_d(t) = 1 - F_d(t)$. It can be derived as:

$$\bar{F}_d(t) = \sum_{j=1}^{J} \omega_j \Big(\sum_{l=0}^{\alpha_j - 1} \frac{(\alpha_j\beta_j t)^l}{l!} e^{-\alpha_j\beta_j t}\Big).$$



(a): Rekeying cost vs ϕ_{th}, where λ=50, and $\frac{1}{\theta}$=500.

(b): Rekeying cost vs ϕ_{th}, where λ=50, and $\frac{1}{\theta}$=1000.

Fig. 8. Rekeying cost for UE when various ϕ_{th} values are applied.

Eq. (23) is rewritten as:

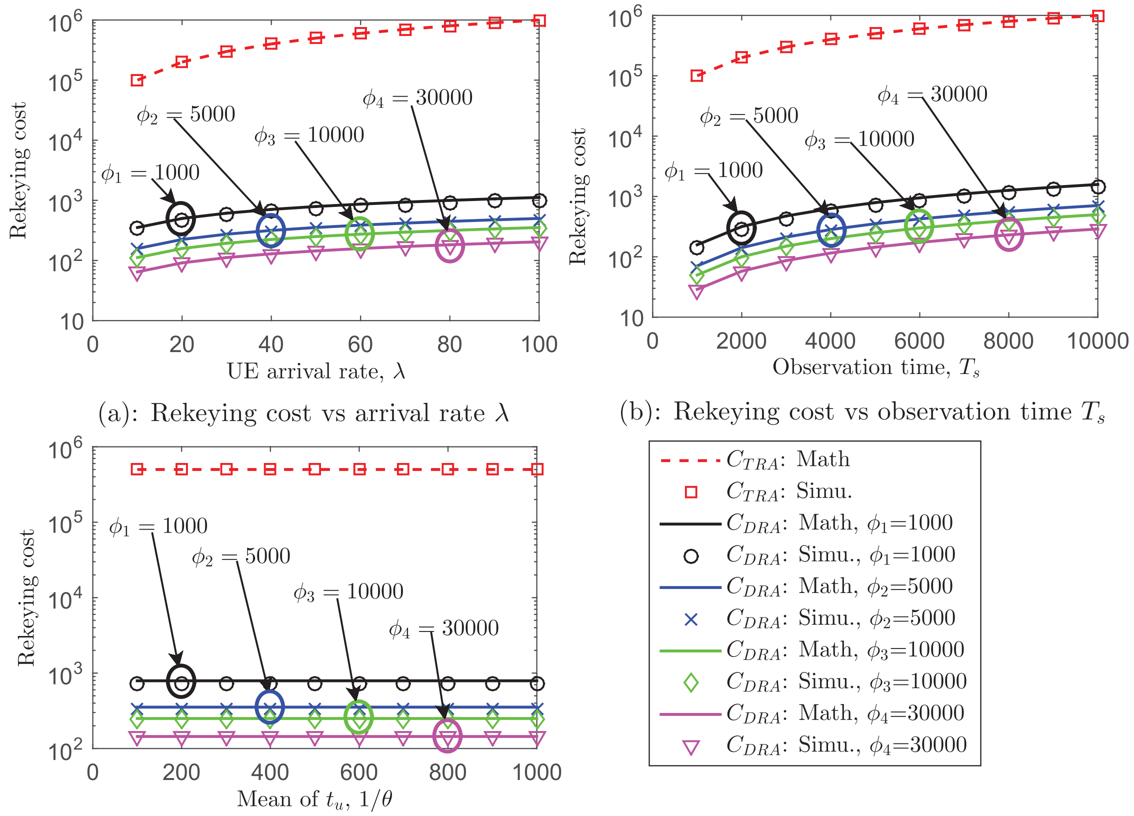
$$\begin{aligned} &p_{DRA} \\ &= 1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \Bigg[1 - \sum_{j=1}^{J} \omega_j \Bigg(\sum_{l=0}^{\alpha_j - 1} \frac{(\alpha_j\beta_j t)^l}{l!} e^{-\alpha_j\beta_j t}\Bigg)\Bigg]dt \\ &= \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \sum_{j=1}^{J} \omega_j \Bigg(\sum_{l=0}^{\alpha_j - 1} \frac{(\alpha_j\beta_j t)^l}{l!} e^{-\alpha_j\beta_j t}\Bigg)dt. \end{aligned} \tag{28}$$

Eq. (24) is then rewritten as:

$$\begin{aligned} \mathcal{N}_{DRA} &= \frac{\omega\lambda T_s}{\theta}\sqrt{\frac{\lambda}{2\phi_{th}}} \\ &\quad \times \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \sum_{j=1}^{J} \omega_j \Bigg(\sum_{l=0}^{\alpha_j - 1} \frac{(\alpha_j\beta_j t)^l}{l!} e^{-\alpha_j\beta_j t}\Bigg)dt. \end{aligned} \tag{29}$$

c) Erlang distribution: The CDF of Erlang distribution is $F_d(t) = 1 - \sum_{n=0}^{\pi - 1} \frac{1}{n!} e^{-\frac{t\pi}{\tau}} (\frac{t\pi}{\tau})^{\pi}$. Eqs. (23) and (24) are rewritten as:

$$\begin{aligned} p_{DRA} &= 1 - \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \Bigg[1 - \sum_{n=0}^{\pi - 1} \frac{1}{n!} e^{-\frac{t\pi}{\tau}} (\frac{t\pi}{\tau})^{\pi}\Bigg]dt \\ &= \sqrt{\frac{\lambda}{2\phi_{th}}} \int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}} \sum_{n=0}^{\pi - 1} \frac{1}{n!} e^{-\frac{t\pi}{\tau}} (\frac{t\pi}{\tau})^{\pi} dt, \end{aligned} \tag{30}$$



(a): Rekeying cost vs arrival rate λ

(b): Rekeying cost vs observation time T_s

(c): Rekeying cost vs mean of t_u, $\frac{1}{\theta}$

Fig. 9. (a), (b), and (c) show the rekeying cost for CN.

and

$$\mathcal{N}_{DRA} = \frac{\omega\lambda T_s}{\theta}\sqrt{\frac{\lambda}{2\phi_{th}}}\int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}}\sum_{n=0}^{\pi-1}\frac{1}{n!}e^{-\frac{t\pi}{\tau}}(\frac{t\pi}{\tau})^{\pi}dt, \qquad (31)$$

respectively.

d) Exponential distribution: The CDF of exponential distribution is $F_d(t) = 1 - e^{-\frac{1}{\tau}t}$. Eq. (23) is rewritten as:

$$\begin{aligned} p_{DRA} &= 1 - \sqrt{\frac{\lambda}{2\phi_{th}}}\int_{t=0}^{\sqrt{\frac{2\phi_{th}}{\lambda}}}\left(1 - e^{-\frac{1}{\tau}t}\right)dt \\ &= \tau\sqrt{\frac{\lambda}{2\phi_{th}}}\left(1 - e^{-\frac{1}{\tau}\sqrt{\frac{2\phi_{th}}{\lambda}}}\right). \qquad (32) \end{aligned}$$

Eq. (24) is then rewritten as:

$$\mathcal{N}_{DRA} = \frac{\omega\lambda\tau T_s}{\theta}\sqrt{\frac{\lambda}{2\phi_{th}}}\left(1 - e^{-\frac{1}{\tau}\sqrt{\frac{2\phi_{th}}{\lambda}}}\right). \qquad (33)$$

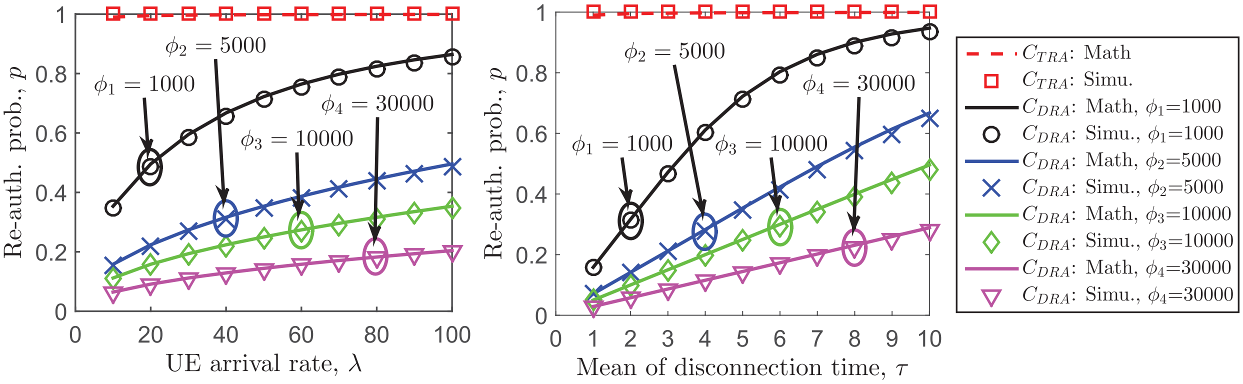
V. Simulation and Numeric Results

The analysis presented in Section IV can quantify the performance of the proposed DRA. It also provides a systematic way for operators and content providers to choose different parameters. The analysis was validated by extensive simulations by using ns-2, version 2.35 [22] with the following simulation settings: $T_s = 5000$ sec, $t_u = 500$ sec, $\tau = 5$ sec, $\lambda = 50$, and $\omega = 0.005$ (see Table I for details). In Figs. 9, 10, and 11, the solid/dashed lines denote the analytical results while the simulation results are presented by small squares, cycles, x-marks, diamonds, and triangles. The simulations were conducted with 98% confidence level. However, the confidence intervals are not drawn here because they are too small and will overlap with other lines and cycles significantly which will make the figures difficult to read.

To identify whether the system enters steady state, in our simulations, we used a time window, $t_w = 100$s, to compute the average UE departure rate λ_d and the average UE arrival rate λ in the time window t_w. Once $\frac{\lambda_d}{\lambda} \geq 98\%$ continually for 100 sec, we considered that the system entered steady state and started to record simulation data. Here, the purpose of t_w is to combat against the randomness of λ and λ_d.

A. Rekeying Cost for UE

We first investigate how the rekeying cost for UE is affected by the threshold of accumulated free enjoy time, ϕ_{th}. We compare the performance of TRA and DRA with different ϕ_{th} values. Fig. 8 illustrates the comparison results. We can see that DRA significantly decreases the rekeying cost for UEs. Please note the y-axis in Fig. 8 is logarithmic scale. Another observation is that by using DRA, rekeying cost for UE decreases as ϕ_{th} becomes bigger. For example, the UE rekeying cost drops to 0.158% when DRA is applied with ϕ_{th}=1000, λ=50, and $\frac{1}{\theta}$=1000. Moreover, when ϕ_{th} rises from 1000 to 30000, the UE rekeying cost further drops by 18.26%.



(a): Re-authen. prob., p vs arrival rate λ (b): Re-authen. prob., p vs τ

Fig. 10. (a) and (b) illustrate the re-authentication probability when a UE is in off-line period.

It demonstrates that adopting DRA with various ϕ_{th} values can easily adjust the rekeying cost for UEs.

B. Rekeying Cost for Core Network

Figs. 9 (a), (b), and (c) show both the analytical and simulation results of the rekeying cost for CN in an eMBMS session in terms of UE arrival rate λ and an observation time interval T_s. In addition, we plot both the analytical and simulation results of DRA by considering the accumulated free enjoying time threshold factor ϕ_{th} with respect to 1000, 5000, 10000, and 30000, respectively. We observe that the rekeying cost of DRA is much lower than that of TRA. For instance, the rekeying cost of DRA is only 3.4% of the rekeying cost of TRA when $\phi_{th} = 1000$ and $\lambda = 100$, meaning that DRA is especially suitable for the case that bursty UE arrival/departure happens. By adjusting ϕ_{th}, operators can easily control the rekeying load for CN using Eq. (15).

As shown in Fig. 9(a), the more UEs join the eMBMS session, the higher the rekeying cost is. The reason is that when a UE joins the eMBMS session, it may stay in the session for a time t_u to enjoy the eMBMS service and then leaves the session. Once the system enters steady state, in an observation time interval the number of UEs joining the session is equal to the number of UEs leaving (as discussed in Section IV-B). In other words, the UE arrival rate equals the UE departure rate, $\lambda = \lambda_d$. As a result, when λ increases, λ_d also increases, causing higher rekeying cost.

Moreover, the design rationale of DRA is to fit for large eMBMS service groups. Generally speaking, eMBMS service groups with a large number of UEs usually come with frequent UE leavings/departures, i.e., great λ and λ_d. Since large λ and λ_d lead to high rekeying cost for CN, our design of DRA is to combat against the impact of large λ and λ_d. Fig. 9(a) shows that, as λ increases, the rekeying cost of DRA increases much slower[3] than the rekeying cost of TRA with different ϕ_{th} values. This validates our design rationale: DRA is scalable to large eMBMS service groups.

We also depict the impact of the observation time interval T_s on the rekeying cost for CN in Fig. 9(b). We observe that both the rekeying cost of TRA and DRA increase linearly when T_s increases (look like exponentially increases due to logarithmic Y-axis). Fig. 9(b) also shows that the rekeying cost of DRA is much lower than that of TRA.

As derived in Eqs. (8) and (15), they demonstrate that the UE staying time t_u has no impact on the rekeying cost of TRA and the rekeying cost of DRA for CN when the system is in steady state. Fig. 9(c) validates this point: when t_u increases from 100 to 1000, all the curves of TRA and DRA are horizontal.

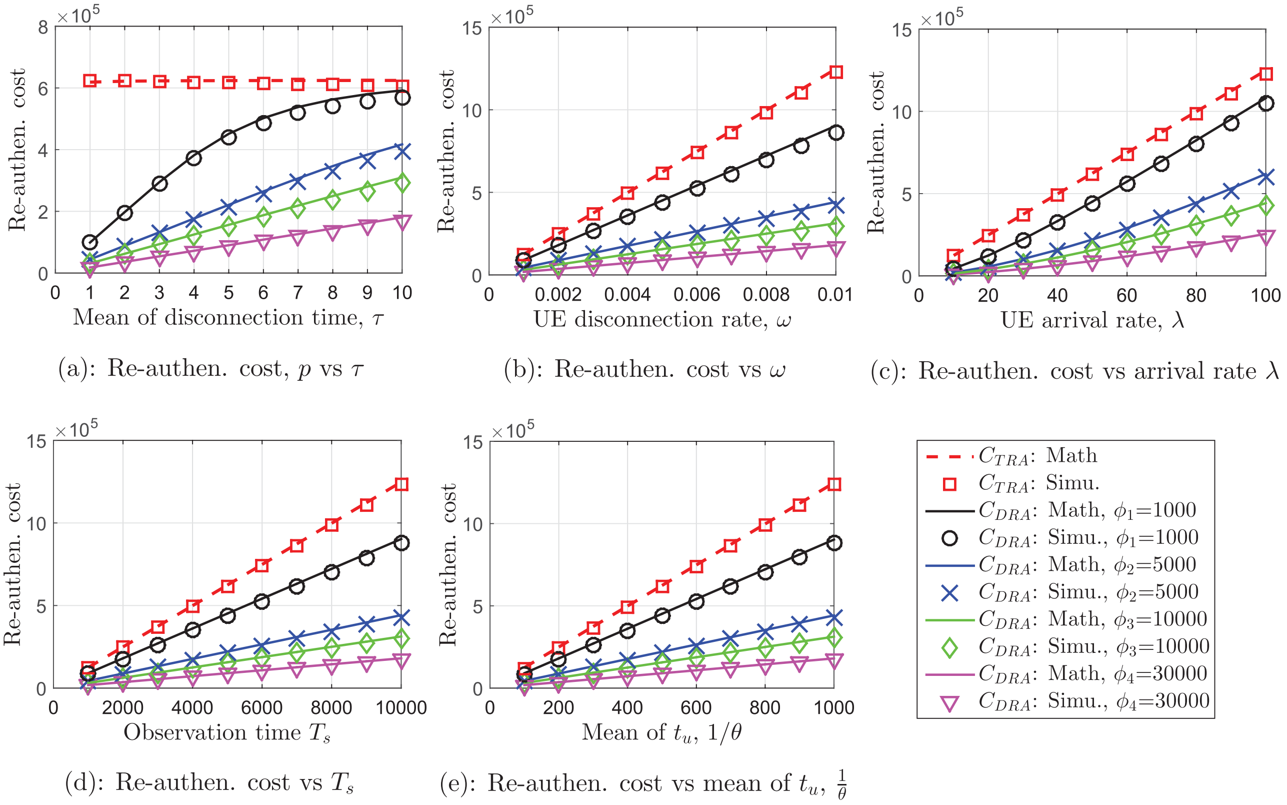
In conclusion, DRA serves as an appropriate analytical model for mobile operators to select a suitable ϕ_{th} to adjust rekeying load for CN. It is also resilient to the impact of quick increasing of UE arrival rate and is thus scalable to large eMBMS service groups. In addition, adopting DRA with various ϕ_{th} values can reduce CN load significantly.

C. Re-Authentication Probability

In this section, we study the re-authentication probability when a UE disconnects from the CN. The impact of UE arrival rate λ on re-authentication probability p is shown in Figs. 10(a) and (b). In these simulations, λ is scaled from 10 to 100. We can see that the re-authentication probability of TRA, p_{TRA}, is almost 100% when λ increases from 10 to 100. This indicates that in the simulation setting[4] once a UE is off-line, it needs to perform re-authentication with almost 100%. It may cause huge re-authentication load for CN if the number of off-line UEs and the frequency of off-line UEs are large. In contrast, the re-authentication probabilities of DRA, p_{DRA}, are much lower than those of TRA. Intuitively, UEs get less chance to perform re-authentication meaning that less re-authentication load for CN. We also observe that p_{DRA} increases when λ becomes larger as shown in Figs. 10(a) and (b). The reason is that larger λ causes higher rekeying rate for both TRA and DRA. Once rekeying happens when a UE is in off-line period, the UE cannot get new key(s) distributed in its off-line interval. Thus, the UE has

[3] Please note that Y-axis is logarithmic scale.

[4] p_{TRA} can be less than 100% if the disconnection time, t_d, and rekeying rate, λ_R, are set as very small values.



(a): Re-authen. cost, p vs τ

(b): Re-authen. cost vs ω

(c): Re-authen. cost vs arrival rate λ

(d): Re-authen. cost vs T_s

(e): Re-authen. cost vs mean of t_u, $\frac{1}{\theta}$

Fig. 11. Re-authentication cost for CN.

to re-authenticate itself to get the newest key as discussed in Section IV-B.

We next investigate how p_{DRA} outperforms p_{TRA} in terms of the mean value of UE disconnection time τ by changing τ from 1s to 10s. The results are shown in Fig. 10(b). One interesting result is that the gap between p_{TRA} and p_{DRA} is big when τ is small. It demonstrates that DRA is especially suitable for short-term disconnections. Similarly, we observe that p_{DRA} becomes larger when τ increases. This is due to the fact that larger disconnection time τ means higher probability that rekeying happens in the disconnection time. Indeed, given a long enough disconnection interval, all UEs have to perform re-authentication no matter TRA or DRA are used. 3GPP has defined a timer for such scenarios in [1], [2], and [6], which is out of scope of this paper.

We conclude that DRA outperforms TRA with respect to re-authentication probability. Both analytical and simulation results show that DRA is especially suitable when short-term unintended disconnection happens frequently. Moreover, we demonstrate that DRA also outperforms TRA in terms of UE arrival rate λ. However, when λ is extremely high and/or τ is very long, p_{DRA} may also approach to 100%. One solution is to increase ϕ_{th} based on Eq. (25) to obtain satisfied re-authentication probability for UEs when different distributions of t_u are applied. Figs. 10(a) and (b) also validate that when ϕ_{th} increases, p_{DRA} becomes smaller.

D. Re-Authentication Cost

For a better illustration of re-authentication cost caused by UE off-line effect, we investigate the re-authentication cost for CN. The results are shown in Figs. 11(a)-(e). We can see that DRA always achieves lower re-authentication cost for CN than that in TRA. Increasing the accumulated free enjoy time threshold ϕ_{th} leads to more benefits on re-authentication load for CN. The curve of re-authentication cost of TRA is horizontal because its re-authentication probability is almost 100%. However, Fig. 11(a) shows that the difference between them dwindles when the mean value of disconnection time τ becomes larger. The reason is that larger τ will lead to higher probability that rekeying happens within it. Similarly, we can adjust ϕ_{th} to decrease re-authentication cost based on Eq. (26) when various distribution of t_u are applied.

We next compare the performance of TRA and DRA with re-authentication cost for CN by inspecting Figs. 11(b)-(e). By a significant margin, DRA outperforms TRA with respect to re-authentication cost for CN. This is validated by both analytical and simulation results in terms of UE disconnection rate ω, UE arrival rate λ, the observation time interval T_s, and the mean value of UE staying time t_u.

Overall, by comparing Figs. 11(a)-(e), DRA significantly outperforms TRA in terms of re-authentication probability for UEs and re-authentication cost for CN.

VI. Optimal DRA

In this section, we discuss the selection of ϕ_{th} for DRA. Recall that we have validated the correctness of the proposed analytical model in Section V. Mobile operators then can plan and design their network optimization strategies. In particular, selecting a suitable free enjoy time threshold ϕ_{th} to balance the security-performance tradeoff is important.

According to Eq. (15), we observe that C_{DRA} is a function of ϕ_{th}. A larger ϕ_{th} means fewer rekeying, i.e., less C_{DRA}. Meanwhile, some revenue will lost due to larger free enjoy time, and vice versa. Thus, we formulate the objective function as:

$$\begin{aligned}&\underset{\phi_{th}}{\text{minimize}}\ F = w_1 C_{DRA} + w_2 \phi_{th},\\ &\text{subject to } 0 < \phi_{th} \le \hat{\phi},\end{aligned} \tag{34}$$

where $\hat{\phi}$ is the upper bound of ϕ, which can be determined by content providers according to their business policies. The coefficients of w_1 and w_2 denote the weighting factors for C_{DRA} and ϕ_{th}, respectively. Increasing w_1 (or w_2) emphasizes more on C_{DRA} (or ϕ_{th}). Here, we do not specify either w_1 or w_2 because such a value should be determined by mobile operators and should take management policies into consideration. In addition, since C_{DRA} has been derived in Eq. (15), the optimal value of ϕ_{th} can be found by solving the differential equation $F' = 0$ and checking the boundary values, i.e., when $\phi_{th} = 0$ and $\phi_{th} = \hat{\phi}$ in F.

VII. Related Work

Previous studies [23]–[27] have addressed the security-performance tradeoff in wireless networks. In [26], the authors addressed the tradeoff between security and throughput in encryption-based wireless security and developed detailed mathematical models to capture the security-throughput tradeoff. The proposed scheme significantly improves the performance compared with traditional approaches. The authors of [27] presented the first work investigating the tradeoff between the achievable throughput and the allowable number of eavesdroppers in a large wireless network. The work well demonstrated that the wireless network can tolerate a single eavesdropper with upper bound attack strength. The authors of [25] studied the tradeoff between routing security and performance on selecting a routing path in multihop wireless networks. The authors derived a multipath routing protocol maximizing the worst-case packet delivery ratio while limiting the worst-case security risk under given threshold. In [23], the authors analyzed the coexistence of security mechanisms and Quality of Service (QoS) mechanisms in resource-constrained wireless networks. A novel dependency-based model was proposed to study the security and QoS tradeoff. The authors of [24] proposed a new dynamic security system architecture that weights the tradeoff between resources, costs and risks for considering the network security profile to optimize the performance of communication networks. The proposed dynamic system allows a better utilization of network resource and save investments in infrastructure. The authors of [28] stated that handover key can be threaten due to rogue base station attacks and formalizes the problem as a tradeoff between signaling load and security key exposure. A detailed mathematical model is derived for a network operator to select an optimal key update interval that fits best with their network management policies.

Despite of the aforementioned studies, the security-performance tradeoff between security of multimedia content, UE signaling overhead, and CN authentication cost were not taken into consideration in eMBMS.

VIII. Conclusions

In this paper, we propose a dynamic rekeying algorithm called DRA to reduce UE signaling overhead and CN authentication cost caused by frequent rekeying with slight compromise of the interest of content providers. We develop analytical and simulation models to investigate the signaling overhead of a UE, C, authentication cost of the CN, $\mathcal{N}$, and revenue loss of a content providers, ϕ. Our performance study provides theoretical guidances and a systematic way for network operators to configure rekeying time interval. When UE arrival/departure rate is higher, the proposed DRA can work more effectively in terms of reducing UE signaling overhead and CN authentication cost.

References

[1] *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall Description, Stage 2, Release 12*, document 3GPP TS 36.300 V12.3.0, Sep. 2014.

[2] *Multimedia Broadcast/Multicast Service (MBMS), Architecture and Functional Description, Release 12*, document 3GPP TS 23.246 V12.3.0, Sep. 2014.

[3] *Multimedia Broadcast/Multicast Service (MBMS), Release 12*, document 3GPP TS 22.146 V12.0.0, Oct. 2014.

[4] *Multimedia Broadcast/Multicast Service (MBMS) User Services, Stage 1, Release 12*, document 3GPP TS 22.246 V12.0.0, Oct. 2014.

[5] *Introduction of the Multimedia Broadcast/Multicast Service (MBMS) in the Radio Access Network (RAN), Stage 2, Release 12*, document 3GPP TS 25.346 V12.0.0, Mar. 2014.

[6] *3G security, Security of Multimedia Broadcast/Multicast Service (MBMS), Release 12*, document 3GPP TS 33.246 V12.0.0, Sep. 2014.

[7] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 8–20, Oct. 2007.

[8] J. Chen, M. Chiang, J. Erman, G. Li, K. K. Ramakrishnan, and R. K. Sinha, "Fair and optimal resource allocation for LTE multicast (eMBMS): Group partitioning and dynamics," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 1266–1274.

[9] *Generic Authentication Architecture (GAA), Generic Bootstrapping Architecture (GBA)*, (Release 13), Standard no. 3GPP TS 33.220 V13.0.0, Jan. 2016.

[10] S.-M. Cheng, W.-R. Lai, P. Lin, and K.-C. Chen, "Key management for UMTS MBMS," *IEEE Trans. Wireless Commun.*, vol. 7, no. 9, pp. 3619–3628, Sep. 2008.

[11] J. Arkko, E. Carrara, F. Lindholm, K. Norrman, and M. Naslund, *MIKEY: Multimedia Internet Keying*, document RFC 3830, Aug. 2004.

[12] Y. Sun *et al.*, "The case for P2P mobile video system over wireless broadband networks: A practical study of challenges for a mobile video provider," *IEEE Netw.*, vol. 27, no. 2, pp. 22–27, Mar. 2013.

[13] D. A. Lyons, "Internet policy's next frontier: Usage-based broadband pricing," *Federal Commun. Law J.*, vol. 66, no. 1, pp. 1–44, 2013.

[14] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Advances in Cryptology—-EUROCRYPT*. New York, NY, USA: Springer-Verlag, 2003, pp. 294–311.

[15] S. M. Ross, *Introduction to Probability Models*, 10th ed. San Francisco, CA, USA: Academic, 2009.

[16] D. Gross, *Fundamentals of Queueing Theory*. New York, NY, USA: Wiley, 2008.

[17] F. P. Kelly, *Reversibility and Stochastic Networks*. New York, NY, USA: Wiley, 1979.

[18] Y. Fang and I. Chlamtac, "Teletraffic analysis and mobility modeling of PCS networks," *IEEE Trans. Commun.*, vol. 47, no. 7, pp. 1062–1072, Jul. 1999.

[19] C. Jedrzycki and V. C. M. Leung, "Probability distribution of channel holding time in cellular telephony systems," in *Proc. IEEE 46th Veh. Technol. Conf. Mobile Technol. Human Race*, Atlanta, GA, USA, May 1996, pp. 247–251.

[20] L. Kleinrock, *Queueing Systems: Theory*, vol. 1. New York, NY, USA: Wiley, 1975.

[21] G. Latouche, V. Ramaswami, and V. G. Kulkarni, "Introduction to matrix analytic methods in stochastic modeling," *J. Appl. Math. Stochastic Anal.*, vol. 12, no. 4, pp. 435–436, 1999.

[22] (Oct. 2016). *The Network Simulator–ns-2*. [Online]. Available: http://www.isi.edu/nsnam/ns/

[23] A. Nieto and J. Lopez, "Analysis and taxonomy of security/QoS tradeoff solutions for the future Internet," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2778–2803, 2014.

[24] K. Y. Youssef, H. Kamel, A. A. Hafez, and A. H. A. Zekry, "On balance between security and performance for LTE wireless networks," in *Proc. IEEE 22nd Int. Conf. Comput. Theory Appl. (ICCTA)*, Oct. 2012, pp. 60–65.

[25] L. Chen and J. Leneutre, "On multipath routing in multihop wireless networks: Security, performance, and their tradeoff," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, p. 6, Feb. 2009.

[26] M. Haleem, C. Mathur, R. Chandramouli, and K. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 313–324, Oct. 2007.

[27] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity tradeoff in large wireless networks using keyless secrecy," in *Proc. 11th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2010, pp. 21–30.

[28] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

Yi Ren (S'08–M'13) received the Ph.D. degree in information communication and technology from the University of Agder, Norway, in 2012. He has been an Assistant Researcher with National Chiao Tung University, Taiwan, since 2012. His current research interests include security and performance analysis in wireless sensor networks, ad hoc, and mesh networks, LTE, smart grid, and e-health security. He received the Best Paper Award at IEEE MDM 2012.

Jyh-Cheng Chen (S'96–M'99–SM'04–F'12) received the Ph.D. degree from the State University of New York at Buffalo, Buffalo, NY, USA, in 1998.

He was a Research Scientist with Bellcore/Telcordia Technologies, Morristown, NJ, USA, from 1998 to 2001, and a Senior Scientist with Telcordia Technologies, Piscataway, NJ, USA, from 2008 to 2010. He was with the Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan, as an Assistant Professor, an Associate Professor, and a Professor from 2001 to 2008. He was also the Director of the Institute of Network Engineering, National Chiao Tung University (NCTU), Hsinchu, from 2011 to 2014. He has been a faculty member of NCTU since 2010. He is currently a Distinguished Professor with the Department of Computer Science, NCTU. He is also serving as the convener, with the Computer Science Program, Ministry of Science and Technology, Taiwan.

Dr. Chen is also a Distinguished Member of the ACM. He is also a member of the Fellows Evaluation Committee, the IEEE Computer Society, in 2012 and 2016, respectively. He received numerous awards, including the Excellent Teaching Award from NCTU, the Outstanding I. T. Elite Award, Taiwan, the Mentor of Merit Award from NCTU, the K. T. Li Breakthrough Award from the Institute of Information and Computing Machinery, the Outstanding Professor of Electrical Engineering from the Chinese Institute of Electrical Engineering, the Outstanding Research Award from the Ministry of Science and Technology, the Outstanding Teaching Award from NTHU, the Best Paper Award for Young Scholars from the IEEE Communications Society Taipei and Tainan Chapters, and the IEEE Information Theory Society Taipei Chapter, and the Telcordia CEO Award.

Jui-Chih Chin received the M.S. degree from the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan, in 2014. He is currently an LTE Modem Software Engineer with MediaTek Inc., Hsinchu, Taiwan. His research interests include mobility management, admission control, resource management, and performance analysis of wireless networks.

Yu-Chee Tseng (S'91–M'95–SM'03–F'12) received the Ph.D. degree in computer and information science from The Ohio State University in 1994. He was the Chairman with the College of Computer Science, National Chiao-Tung University, Taiwan, from 2005 to 2009. He has been the Dean with the College of Computer Science, National Chiao-Tung University, since 2011.

He was the Y. Z. Hsu Scientific Chair Professor from 2012 to 2013. He has been the NCTU Chair Professor since 2011. His research interests include mobile computing, wireless communication, and Internet of Things. He received the Outstanding Research Award (National Science Council, 2001, 2003, and 2009), the Best Paper AAward (IntâŁ™ Conf. on Parallel Processing, 2003), the Elite I. T. Award in 2004, and the Distinguished Alumnus Award (Ohio State University, 2005), and the Y. Z. Hsu Scientific Paper Award in 2009. He served/serves on the editorial boards of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE INTERNET OF THINGS JOURNAL. His h-index is over 60.