Impacts of S1 and X2 Interfaces on eMBMS Handover Failure: Solution and Performance Analysis

Yi Ren, Jyh-Cheng Chen, *Fellow, IEEE*, and Jui-Chih Chin

***Abstract*—In evolved Multimedia Broadcast/Multicast Service (eMBMS), service continuity enables users move from one cell to another without interrupting eMBMS service. Unlike traditional handover in unicast transmission, a UE can receive eMBMS service in either unicast or multicast mode. In this paper, we point out a new handover failure problem in eMBMS due to the miss of rekeying information. We first take a close look at the new handover scenarios. We then investigate the problem by using comprehensive mathematical models. Our models provide insights on the new handover problem and introduce theoretical guidelines for mobile operators to design and optimize their networks without wide deployment to save cost and time. Moreover, we propose a solution to combat against the handover failure. Both the simulation and analytical results demonstrate that the impacts of the eMBMS handover failure are reduced significantly. In this paper, we present a systematic way to investigate the handover failure problem in eMBMS.**

***Index Terms*—mobility, eMBMS handover failure, multicast, performance analysis**

I. Introduction

NOWADAYS, more and more people are switching from watching traditional TV to streaming video on mobile devices. Live streaming apps, such as YouTube Live, Facebook Live, Verizon Go90, attract millions of users. Besides, the number of concurrent live viewers could be huge. For example, on the 3rd U.S. presidential debates in 2016, YouTube Live drew 1.7 million peak *concurrent live* viewers. The 2016 Super Bowl got 111.9 million viewers with an average of 3.96 million viewers on the live streaming [1].

Long-Term Evolution (LTE) Broadcast, also known as evolved Multimedia Broadcast/Multicast Service (eMBMS) [2], was proposed to meet the demand for broadcasting services. LTE Broadcast delivers the *same content* to *a large number* of devices at the *same time*, which significantly reduces transmission cost and increases efficiency of the network. This makes it ideal for live streaming services. In June 2015, BBC R&D and EE demonstrated LTE Broadcast during the FA Cup final in the U.K. In Oct. 2015, Verizon commercially launched Go90 eMBMS service [3]. Verizon customers can purchase a full season of NBA League Pass for USD 99.50 through Go90.

eMBMS enables user mobility by using service continuity feature [2], [4]. Specifically, users with hand-held User Equipment (UE) terminals can enjoy eMBMS services while moving within an *MBMS Single Frequency Network (MBSFN)* service area as shown in Fig. 1. An MBSFN service area usually consists of one or more MBSFN areas, in which a set of evolved NodeBs (eNBs) uses the same resource block to deliver eMBMS services in a time-synchronized manner. In the service area, therefore, users are able to move (*handover*) from one cell (serving eNB) to another (target eNB) without interrupting the MBMS service. However, different from unicast transmission which is used in RRC_Connected state only, a UE can receive eMBMS services in either RRC_Connected state or RRC_Idle state [4]. Due to this characteristic, in this paper, we point out an eMBMS service continuity failure problem, referred to as *eMBMS Handover Failure*[1].

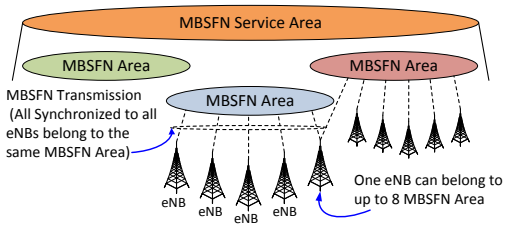

Fig. 1: An example of the relationship between eNBs, MBSFN areas, and MBSFN service areas.

The eMBMS Handover Failure problem[2] is caused mainly because of missing the rekeying information. In particular, data security is one of the essential requirements for eMBMS. To prevent unauthorized users from accessing eMBMS contents, 3GPP introduces Key Management Mechanism (KMM) [5]. Its basic idea is to maintain a multicast group, in which only UEs belonged to the same group can receive the multicast data [6]. When a member joins/leaves the group, a group key needs to be updated to add/revoke the member. The process is referred to as *rekeying*. As a result, the users holding the *old keys* are unable to access the subsequent contents.

Given the fact that users with old keys are unable to access subsequent eMBMS contents, any key material missing may cause encryption/ciphering mismatch, leading to the eMBMS handover failure. In unicast transmission, if any message fails to be transmitted, a re-transmission attempt can be conducted when a UE stays in RRC_Connected state. In eMBMS, a UE can receive eMBMS service in RRC_Idle state in which no dedicated network resource is maintained between the UE and the core network. In other words, there is no ACK mechanism to confirm the messages received. Also, when a UE receives eMBMS service in RRC_Connected state, the updated key material is unicast to every UE joined the eMBMS services over UDP, in which there is no retransmission. The core

Y. Ren is with the School of Computing Science, University of East Anglia (UEA), Norwich, UK. He was with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. E-mail: e.ren@uea.ac.uk.

J.-C. Chen is with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. e-mail: jcc@cs.nctu.edu.tw

J.-C. Chin was with MediaTek Inc., Hsinchu, Taiwan. e-mail: wayne62109@gmail.com

[1]Please note that there is no handover process when a UE is in RRC_Idle state. We use the handover to denote the moving behavior across cells.

[2]For simplicity, we simply call it as *Handover Failure* problem in rest of the paper.

network will still update the group key even if some of the UEs do not receive the rekeying information correctly [4], [5]. *Therefore, those UEs missing the rekeying information will not be able to derive new keys. Their rekeying procedure will be stopped, which results in Handover Failure (to be detailed in Section III).*

Mobility management is a major challenge in cellular networks. Extensive studies [7]–[15] have been conducted to enhance mobility performance as well as to reduce handover failure. However, these studies were not tailored to eMBMS mobility and handover scenario, which cannot be applied to enhance eMBMS service continuity directly. In our earlier work [16], we have addressed the impacts of rekeying interval on eMBMS system performance and the revenue loss of content providers. However, eMBMS handover scenario was ignored.

To the best of our knowledge, we are the first to address the service continuity problem in eMBMS caused by missing rekeying information. In this paper, we first take a close look at the LTE mobility management mechanism and eMBMS KMM. When eMBMS UEs are in RRC_Connected state, deploying X2 interface may reduce handover failure. However, the X2 interface suffers from the following deployment issues. Initially the X2 interface was rarely activated in real-world LTE environments [17]. Although this is starting to change, supporting X2 handover is not easy because of possible *scalability* and *instability* issues [18]. Also, configuring X2 gateway needs to upgrade all eNBs to Release 12 of the standards, which is costly and time-consuming. To protect the investments made in old equipment, cellular operators usually evolve slowly and will not upgrade to a new release immediately. These issues have been an obstacle standing in the way of applying X2 handover in commercial networks [18]. Even though X2 interface is deployed, it may be temporarily unavailable due to no enough bandwidth available in X2 interface or network failure. Also, *X2 interface does not help for eMBMS UEs being in RRC_Idle state*.

So, what is the impact of adding an X2 interface for eMBMS handover on the network performance? Are there any other factors to diminish eMBMS service continuity failure when a UE is in RRC_Idle state? For these issues, we propose a set of analytical models to characterize the eMBMS mobility performance. Based on the analytical models, we have the following insights which are often difficult to obtain without detailed mathematical analysis. We find out that not only X2 interface has impact on handover failure. Other factors, such as session life time, cell residence time, and UE arrival rate, also play some roles. Instead of randomly tuning those factors, based on our findings, we provide theoretical guidelines for operators to design and optimize their networks for mobile eMBMS services. We also analyze the handover failure when there is no X2 interface available for eMBMS handover, i.e., mobility with S1 interface. We have also conducted extensive simulations by using ns2 to validate our mathematical models.

The rest of the paper is organized as follows. Section II introduces background. Section III defines the problem. Section IV reviews the related work. Challenges and our contributions are delineated in Section V. The analytical model

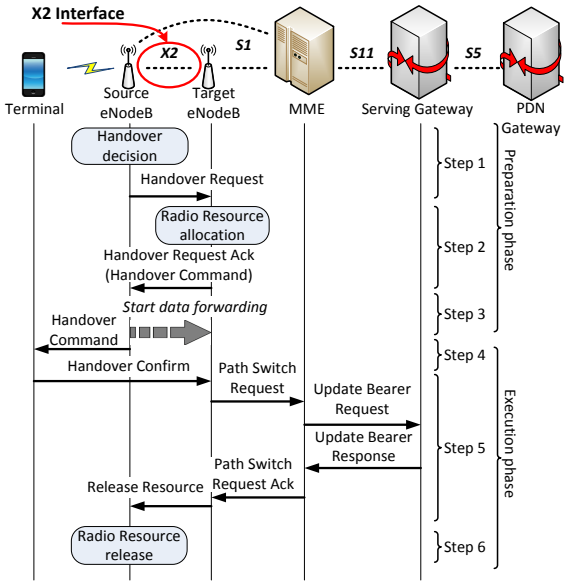

Fig. 2: Intra-E-UTRAN mobility with X2 interface support - message flow.

is presented in Section VI, followed by the numerical results discussed in Section VII. Guidelines for operators then are presented in Section VIII. Section IX summaries this paper.

II. Background

In this section, backgrounds on LTE mobility management [19] and eMBMS KMM [2], [5], [20] are reviewed in Sections II-A and II-B, respectively.

A. LTE Mobility Management

In this paper, we mainly focus on intra-Evolved Universal Terrestrial Radio Access Network (intra-E-UTRAN) active mode mobility which can be categorized as: (a) mobility with X2 support, and (b) mobility without X2 support. They are discussed in the following sessions.

1) Mobility with X2 Support: X2 interface is an interface between eNBs and is used to transmit packets between the eNBs. With the support of X2 interface between source eNB and target eNB, the source eNB is able to forward all downlink Packet Data Units (PDUs) buffered in the Radio Link Control (RLC) buffer upon receiving the *Handover Request ACK* message. By doing this, packet loss during handover procedure may be reduced. Fig. 2 shows the message flows of the handover procedure defined in 3GPP [21] with X2 interface:

- Step 1: Once the source eNB makes the handover decision, it issues Handover Request message to the target eNB.
- Step 2: After all needed resources are allocated, the target eNB answers with the Handover Request ACK message.
- Step 3: Upon receiving the Handover Request ACK message, *the source eNB forwards all the buffered data to the target eNB directly over the X2 interface*.
- Step 4: The source eNB forwards the Handover Command message which is encapsulated in the Handover Request ACK message in Step 2 to the UE.
- Step 5: Once the UE is synchronized with the target eNB, it sends the Handover Confirm message triggering the

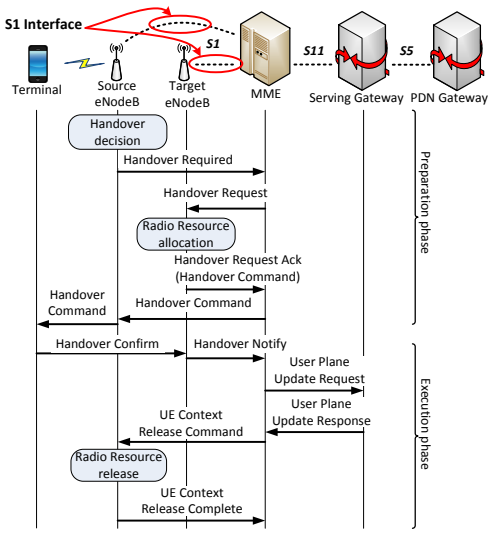

Fig. 3: Intra-E-UTRAN mobility without X2 interface support (also called mobility with S1 interface) - message flow.

Path Switch procedure. This procedure informs Mobility Management Entity (MME) that an intra E-UTRAN handover is successfully completed via X2 interface.

- Step 6: Finally, the radio resources in the Source eNB allocated to the UE are released.

2) Mobility without X2 Support (also called mobility using S1 interface): The main principle of this case is very similar to that in the previous one. The major difference is the absence of the X2 interface. Instead, S1 interface is used for the handover procedure as illustrated in Fig. 3. As a consequence, MME acts as a relay for signaling messages between the source and target eNBs. Therefore, data forwarding procedure in Step 3 in Fig. 2 is not conducted here. Hence, if there are RLC PDUs buffered in the source eNB, *all of them will be lost* when the handover is performed.

3) Summary: In conclusion, the RLC PDUs buffered at the source eNB may be lost. In practical, it may happen because X2 interface is not available between eNBs.

B. Security of Evolved Multimedia Broadcast/Multicast Service (eMBMS)

The eMBMS KMM architecture defined in 3GPP [5] consists of Bootstrapping Server Function (BSF), Broadcast/Multicast Service Center (BM-SC), content provider, eMBMS gateway, and UEs, as shown in Fig. 4. More precisely, BSF is a part of the Generic Bootstrapping Architecture (GBA) which establishes shared secret between UEs and BM-SC. The BM-SC acts as an entry point for content delivery services, and forwards the broadcast/multicast packets to the eMBMS gateway from the content provider. BSF, BM-SC, and eMBMS gateway are within Core Network (CN).

In order to protect eMBMS data, 3GPP defined a set of four security keys in eMBMS KMM [2], [5], which are MBMS Request Key (MRK), MBMS Service Key (MSK), MBMS Traffic Key (MTK), and MBMS User Key (MUK). MRK is mainly used for authentication. MUK secures the distribution of MSK, while MSK is used to protect a certain eMBMS

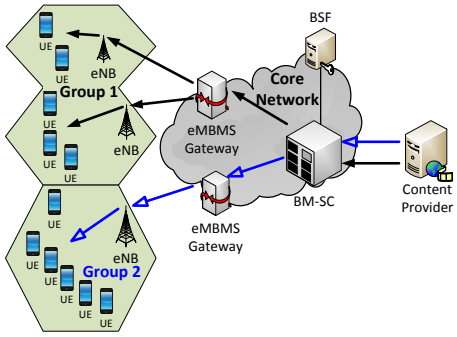

Fig. 4: A simplified example of eMBMS architecture.

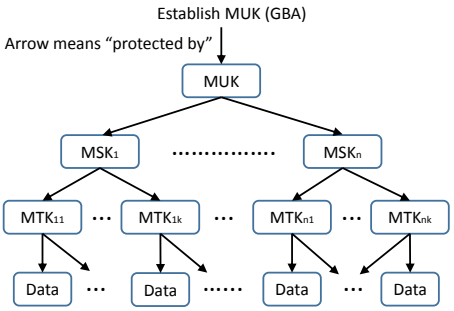

Fig. 5: The relationship between MUK, MSK, MTK, and eMBMS data.

session and the transmission of MTK. MTK is responsible to encrypt and to decrypt eMBMS traffic. In short, MUK, MSK, and MTK are used to protect data (see their relationship in Fig. 5). Here, $\{\text{MSK}_1, \text{MSK}_2, \cdots, \text{MSK}_\text{n}\}$ are a sequence of keys in terms of time. For example, MSK_1 is the previous key of MSK_2. Similarly, MTK_{11} is the previous key of MTK_{12}. For eMBMS service group 1 and group 2 in Fig. 4, different key sets are distributed to them, respectively. For example, $\{\text{MSK}_1^1, \text{MSK}_2^1, \cdots, \text{MSK}_\text{n}^1\}$ are for group 1 and $\{\text{MSK}_1^2, \text{MSK}_2^2, \cdots, \text{MSK}_\text{n}^2\}$ are for group 2. For the sake of simplicity, we did not use the notation MSK^1 and MSK^2 to indicate the keys for the two groups in the paper.

During an eMBMS service session, MSK/MTK is (are) updated (referred to as *rekeying* in this paper) when one of the following events happens: (a) Event 1: a new UE joins the eMBMS session, (b) Event 2: a joined UE leaves the eMBMS session, (c) Event 3: the timer of MSK expires, and (d) Event 4: the timer of MTK expires. In order to update MSK/MTK, User Service Join procedure (for Event 1), User Service Leave procedure (for Event 2), MSK Periodic Update procedure (for Event 3), or MTK Periodic Update procedure (for Event 4) are carried out [2], [5], [22].

Here, we show a simplified example of User Service Join procedure for Event 1 in Fig. 6, where $\text{UE}_{\{1\ldots\text{n}\}}$ denote the UEs which have already joined the service, and $\text{UE}_{\text{n}+1}$ is a new UE.

- Step 1: The new UE, $\text{UE}_{\text{n}+1}$, first sends a service join request to the BM-SC. The BM-SC then will ask $\text{UE}_{\text{n}+1}$ to initiate the bootstrap authentication procedure with the BSF.
- Step 2: The $\text{UE}_{\text{n}+1}$ performs the bootstrapping authentication procedure with the BSF and derives its $\text{MRK}_{\text{n}+1}$

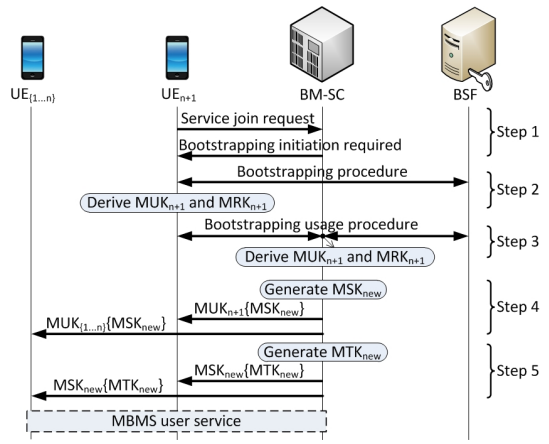

Fig. 6: A new UE joins an eMBMS user service - message flow.

and MUK_{n+1}.

- Step 3: After the UE_{n+1} has derived MRK_{n+1} and MUK_{n+1}, it authenticates itself with the BM-SC using the MRK_{n+1}.
- Step 4: The BM-SC generates a new MSK, MSK_{new}, and *unicasts MIKEY message [23] over UDP* to transport the MSK_{new} to every UE that has joined the service by Dedicated Control Channel (DCCH) and Dedicated Traffic Channel (DTCH) [4], [5]. 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, MTK_{new}, encrypted by MSK_{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) [4], [5].

III. Problem Statement

Due to the requirements of charging and content protection, eMBMS KMM has to guarantee forward security[3]. That is, a UE, which is revoked from the eMBMS service at time t, will not be able to access the encrypted content after time t. A formal definition of forward security is given in Definition 1 [16].

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 the 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.*

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 $\mathcal{K}_i \nRightarrow \mathcal{K}_j$ ($i \geq 1, j \geq i+2$). 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

[3]KMM provides both forward security and backward security. However, backward security is out of the scope of this paper.

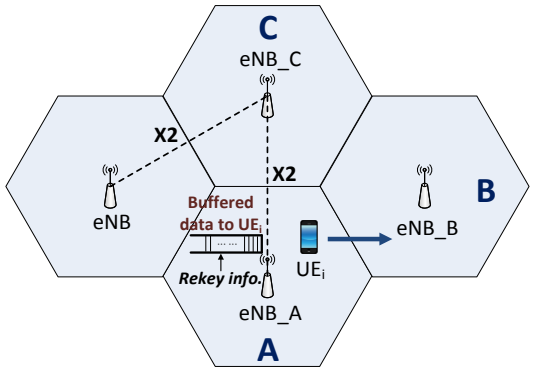

Fig. 7: An example of UE mobility supported by either X2 interface or S1 interface.

UE's perspective. Next, we will use an example to explain the eMBMS handover failure caused by key missing.

As shown in Fig. 7, UEs may move between eNBs within an MBSFN service area. Depending on network conditions[4], RLC PDUs may be buffered in the eNB's buffer for a short period of time [24]. When a UE moves from cell A to cell C, eNB_A will forward buffered RLC PDUs to eNB_C via the X2 interface between them, assuming eNB_A and eNB_C are connected by X2 interface. Whereas, if the UE moves from cell A to cell B where X2 interface is not available between the two eNBs, the RLC PDUs buffered in eNB_A may be lost (to be detailed in the next paragraph). The lost data will lead to eMBMS handover failure if the rekeying information happens to be in it.

To be more specific, the rekeying information may be lost in the following two cases. First, MSK_{new} may be lost due to UDP transmission. Recall that in Step 4 in Fig. 6, the updated MSK_{new} is unicast in MIKEY message to every UE joined the eMBMS services over UDP [4], [5]. There is no ACK to confirm that the UEs have received the updated MSK_{new} correctly [5]. Second, MTK_{new} may be lost during *multicast* transmission. In Step 5 in Fig. 6, the MTK_{new} is multicast to every UE joined the service over UDP [4], [5]. A UE will not send an error message to the BM-SC because of not receiving an MTK message [5]. The eMBMS KMM will still update security keys even if some UEs do not receive the rekeying information correctly.

As a conclusion, 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. 6). Therefore, handover failure will happen if the MIKEY message happens to be in the lost data which is not forwarded from the serving eNB to the target eNB.

IV. Related Work

Approaches aimed to enhance mobility performance have been intensive studied [8]–[16]. In the case of small cells, due to the coverage constrains of small cells, handovers in dense small cells are frequent. The authors in [8] modeled and analyzed the handover failure problem in small cell networks.

[4]Generally speaking, good/bad network condition leads to less/more RLC PDUs buffered in eNBs.

A closed-form expression of the handover failure probability is characterized, which provides key insights into the mobility management problem. The work [9] made theoretical analysis on cross-tier handover in small cell networks based on stochastic geometry approach. The analytical results provide fundamental supports to improve mobility management in small cell networks. The authors in [10] proposed a novel local anchor-based architecture to reduce handover failure in small cells. The authors also derived closed-form expressions of key handover metrics to evaluate the proposed schemes. The authors in [11] studied inter-beam handover scheme for mmWave mobile communication systems. Due to the characteristic of narrow beams, the inter-beam handover is frequent, leading to handover failure and signaling overhead. The proposed scheme decreases handover failure rate and reduces signaling overhead significantly. The authors of [25] proposed a delay timer algorithm to reduce handover cost. An analytical model was derived to study the effects of traffic and user mobility on system performance, which can help cellular operators to plan network more efficiently.

When a UE quickly passes through cells, frequent handovers may lead to serious handover failures. The authors of [12] proposed a multi-RAT soft handover approach to enhance wireless communications on high-speed trains. They showed through detailed analysis that the proposed approach can effectively improve the handover performance in the high-speed train scenario. Reference [13] introduced a novel group in-network handover procedure, which can aggregate similar in-network handover procedures in the core network, and reduce both time and signaling cost during handover. The authors of [14] proposed a set of new handover procedures considering two antennas on the top of a train. The procedure optimizes the utilization of the two antennas and decreases the overhead. It also improves the QoS of the users. Both handover failure probability and communication interruption probability are reduced.

However, none of the above studies [8]–[14] considered the eMBMS handover failure problem due to key update, as discussed in Section III. Perhaps, the closest work to ours was studied in [15] that the impacts of key updates on handover management are taken into consideration. The authors addressed the vulnerability of handover key management and pointed out that periodic updates of the root key are an integral part of handover key management. They then proposed an analytical model to determine an optimal rekey interval to minimize the signaling load. However, handover failure due to key missing was not discussed. In our recent work [16], we introduce that frequent rekeying may lead to eMBMS service failure. However, eMBMS mobility/handover scenario was not considered.

V. Challenges and Contributions

In this section, we summarize the challenges and delineate our contributions.

A. Challenges

1) The RLC PDUs buffered at the source eNB may be lost if X2 interface is not available temporarily or permanently between eNBs. The reasons could be various, such as no enough bandwidth available in X2 interface for eMBMS service, network equipment failure, using legacy network equipment, or simply from the fact that the operator is not willing to deploy X2 connectivity between eNBs due to cost concerns.
2) In eMBMS, the core network will still update the group key even if some of the UEs do not receive the rekeying information correctly. Therefore, those UEs missing the rekeying information will not be able to derive new keys. Their rekeying procedure will be stopped, which results in eMBMS handover failure.
3) The number of UEs in an eMBMS multicast group is usually much more than that in other wireless networks. Besides, in eMBMS, UEs may conduct handovers between eNBs, and enter/exit the eMBMS service randomly and frequently.

B. Contributions

Although eMBMS has been standardized by 3GPP, it is still in trial in most countries. To the best of our knowledge, we are the first to identify the eMBMS handover failure problem caused by eMBMS KMM when a UE performs handover using the legacy S1 interface. As aforementioned discussion, adding X2 interface between eNBs is a straightforward way to solve the problem. In doing so, the following two cases should be taken into consideration by cellular operators.

- Case 1: As discussed in Section I, supporting X2 handover is not easy because of possible scalability and instability issues [18]. Various other issues have also been an obstacle standing in the way of applying X2 handover in commercial networks. Should a cellular operator deploy X2 interface in its existing network? If yes, should a cellular operator deploy X2 interface in the whole network or just in some parts of the network? In particular, what is the impact of X2 interface on network performance in terms of UE handover?
- Case 2: For an existing network, deploying X2 interfaces within a short period of time is not an easy task. For a legacy network with S1 interface only, are there other ways to diminish the impact of handover failure without X2 interface?

Our contributions include:

1) We propose analytical models to answer the questions in Case 1 in Section VI. Based on our analysis, we find out that not only X2 interface has impact on eMBMS handover failure, other factors such as session life time, cell residence time, and UE arrival rate, also play some roles.
2) We propose a solution for Case 2 in Section VIII. If an operator cannot deploy X2 interface due to various reasons, we still can deal with the bursty UE arrivals by adjusting rekeying rate.
3) We provide theoretical guidelines for operators to design and optimize their networks for mobile eMBMS services in Section VIII. We also present a systematic way to investigate the handover failure problem in eMBMS.

TABLE I: List of Parameters

Notation	Unit	Description
t_s	s	Life time of a session
t_{cr}	s	Cell residence time
t_I, t_{I_l}	s	Rekey time interval (spec, ours)
t_r, t_{r_l}	s	Time interval between the UE hands over to next eNB and the first rekeying operation occurs (spec, ours)
t_b	s	Data buffered time interval
t_e	s	Time interval between the new session starts and the first handover take place
$\frac{1}{\mu_s}$, $\frac{1}{\mu_{cr}}$, $\frac{1}{\mu_b}$	s	Mean value of t_s, t_{cr}, t_b
λ_s	1/s	UE arrival rate in a session
λ_r	1/s	Rekeying rate
p_{X2}		The probability of existing an X2 interface between eNBs/HeNBs
p_h		eMBMS handover failure probability
p_c		The probability of a UE's session is completed w/o encountering any failure
p_{nc}		The probability of a UE's session that encounters failure(s)
p_f, p_{f_l}		The probability of rekeying information lost during an S1 handover (spec, ours)
p_{I_l}		The probability mass function (pmf) of prolonged rekeying operation
p_s		The probability of successful handover
f_s, f_{cr}, f_b, f_e		pdf of t_s, t_{cr}, t_b, t_e
f_I, f_{I_l}, f_r, f_{r_l}		pdf of t_I, t_{I_l}, t_r, t_{r_l}
F_b, F_I, F_{I_l}		CDF of t_b, t_I, t_{I_l}

VI. Analytical Model

In this section, novel analytical models are proposed to analyze the impacts of replacing S1 interface with X2 interface in legacy networks. More specifically, a set of performance metrics are proposed and modeled to evaluate the network performance. With the analytical models, cellular operators can quickly obtain the performance for the aforementioned Case 1 to save deployment cost and time. The operators thus are able to design and optimize their networks by using the metrics and analytical models without wide deployment which is too costly and time-consuming. In the analytical models, common properties of the handover failure are addressed. We then propose a solution for Case 2 to diminish the impact of S1 interface on handover failure in eMBMS services in Section VIII.

In the analytical models, we use the commonly used assumptions in cellular networks that both session holding time t_s and cell residence time t_{cr} are assumed to be exponential distributed [16], [26]–[28], with mean value $\frac{1}{\mu_s}$ and $\frac{1}{\mu_{cr}}$, and probability density function (pdf) $f_s(t)$ and $f_{cr}(t)$, respectively. During a session holding time t_s, a UE will visit K cells (with cell residence time t_{cr_i} in i^{th} cell). Because the data for a UE will be buffered at current serving eNB for a short period of time, we assume that the time is t_b, with mean $\frac{1}{\mu_b}$ and pdf $f_b(t)$. The parameters used in the analysis are listed in Table I.

A. Modeling of eMBMS Handover Failure Probability

First, we are interested in the probability, p_h, that rekeying information is lost during a handover, which is referred to as *handover failure* for simplicity in this study. The handover failure probability is one of the most important metrics to evaluate network performance in cellular networks. It is closely related to users' Quality of Experience (QoE), especially for the users with high mobility.

Recall that the rekeying information will be lost during a handover if both the rekeying information is in the buffer of serving eNB and there is no X2 interface between the serving eNB and the target eNB. Hence,

$$p_h = p_f(1 - p_{\text{X2}}), \tag{1}$$

where p_f denotes the probability of missing rekeying information during an S1-based handover (without X2 interface), and p_{X2} is the probability that X2 interface exists between the serving eNB and the target eNB.

As shown in Fig. 8, t_I denotes the time interval between two rekeying operations of MSK/MTK with pdf, $f_I(t)$, and cumulative distribution function (CDF), $F_I(t)$. Let t_r ($t_r < t_I$) denote the time interval between the UE performing handover and the arrival of next rekeying information. It is easy to know that p_f equals to that at least one rekeying information is included in the buffer as discussed in Section III. Therefore, we have:

$$p_f = Pr\{t_b > t_r\} = \int_{t_b=0}^{\infty} \int_{t=0}^{t_b} f_b(t_b) f_r(t) dt dt_b, \tag{2}$$

where $f_r(t)$ is the pdf of t_r. According to the *Excess Life Theorem* [29], we derive $f_r(t)$ as:

$$f_r(t) = \lambda_r \int_{s=t}^{\infty} f_I(s) ds = \lambda_r e^{-\lambda_r t}, \tag{3}$$

where λ_r is the rekey rate. Therefore, from Eq. (3), Eq. (2) is

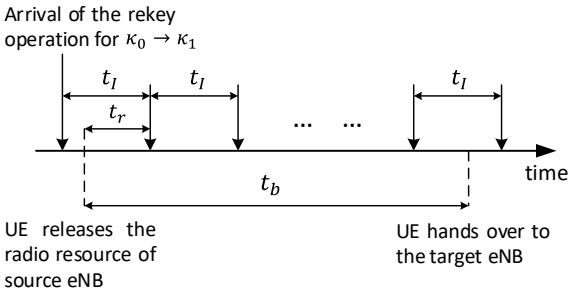

Fig. 8: Relationship between rekeying and buffered data lost.

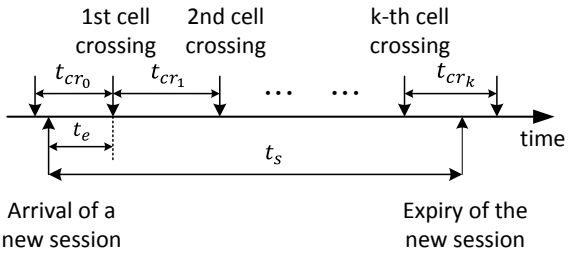

Fig. 9: Timing diagram for the new session arrival and the cell crossing.

rewritten as:

$$p_f = \int_{t_b=0}^{\infty}\int_{t=0}^{t_b} f_b(t_b)\lambda_r e^{-\lambda_r t} dt dt_b = \int_{t_b=0}^{\infty} f_b(t_b)(1-e^{-\lambda_r t_b})dt_b = 1 - f_b^*(\lambda_r). \quad (4)$$

Since the buffered time, t_b, is assumed to be general distribution, here we drive p_f and p_h using three distributions as examples.

Gamma Distribution: The CDF of Gamma distribution, Gamma$(k, \frac{1}{k\mu_b})$, is $F_b(t_b) = \frac{1}{\Gamma(k)}\gamma(k, k\mu_b t_b)$. Also, the Laplace transform of the Gamma pdf is $f_b^*(s) = (1+\frac{s}{k\mu_b})^{-k}$. Hence, p_f is rewritten as $p_f = 1 - \left(1+\frac{\lambda_r}{k\mu_b}\right)^{-k} = 1 - \left(\frac{k\mu_b}{k\mu_b+\lambda_r}\right)^k$, and we then rewrite Eq. (1) as $p_h = \left[1 - \left(\frac{k\mu_b}{k\mu_b+\lambda_r}\right)^k\right](1-p_{\text{X2}})$.

Erlang Distribution: The Laplace transform of Erlang distribution, $Erlang(k, \mu_b)$, is given as $f_b^*(s) = (\frac{\mu_b}{\mu_b+s})^k$. Hence, p_f is rewritten as $p_f = 1 - \left(\frac{\mu_b}{\mu_b+\lambda_r}\right)^k$, and we then rewrite Eq. (1) as $p_h = \left[1 - \left(\frac{\mu_b}{\mu_b+\lambda_r}\right)^k\right](1-p_{\text{X2}})$.

Exponential Distribution: The CDF of Exponential distribution, Exp(μ_b), is $F_b(t_b) = 1 - e^{-\mu_b t_b}$, and the Laplace transform of the exponential pdf is $f_b^*(s) = \frac{\mu_b}{\mu_b+s}$. Hence, p_f is rewritten as $p_f = \frac{\lambda_r}{\mu_b+\lambda_r}$, and we then rewrite Eq. (1) as $p_h = \left[\frac{\lambda_r}{\mu_b+\lambda_r}\right](1-p_{\text{X2}})$.

p_f and p_h are very important factors to model the performance metrics in this study. We have derived p_f and p_h based on Gamma distribution, Erlang distribution, and Exponential distribution, respectively. In the following sections, we will use Gamma distribution as an example for p_f and p_h, that is, $p_f = 1 - \left(\frac{k\mu_b}{k\mu_b+\lambda_r}\right)^k$ and $p_h = \left[1 - \left(\frac{k\mu_b}{k\mu_b+\lambda_r}\right)^k\right](1-p_{\text{X2}})$. The reasons are twofold. One is due to the page limit. The other reason is that the distribution of any positive random variable can be approximated by a combination of Gamma distribution as stated in Lemma 3.9 in [30].

B. Modeling of eMBMS Session Failure Probability

The eMBMS session failure probability, p_{nc}, denotes the probability that a UE's eMBMS service session is forced to be terminated[5]. It is used to evaluate the QoE of eMBMS users.

We first derive $p_c = 1 - p_{nc}$, the probability that a session completes successfully (without handover failures):

$$\begin{aligned} p_c &= \sum_{k=0}^{\infty} Pr\{\text{visit } k \text{ cells}\} \\ &\quad \times Pr\{\text{session completed successfully}|\text{visit } k \text{ cells}\} \\ &= \sum_{k=0}^{\infty} Pr\{K=k|T_s=t_s\}\cdot p_s^k\,, \end{aligned} \quad (5)$$

where p_s is the probability of successful handover with X2 interface. Recall that in such conditions, rekeying information will not be lost during the handover due to the data forwarding via X2 interface. We have:

$$p_s = 1 - p_h = f_b^*(\lambda_r) + p_{\text{X2}} - f_b^*(\lambda_r)\cdot p_{\text{X2}}. \quad (6)$$

Let $Pr\{K=k|T_s=t_s\}$ be the probability that a UE visits k ($k \geq 1$) cells within the session. In each cell, UE stays for a time interval, t_{cr}, which is assumed to be exponentially distributed with Laplace transform $f_{cr}^*(s) = \frac{\mu_{cr}}{\mu_{cr}+s}$. As shown in Fig. 9, it is easy to know that $Pr\{K=k|T_s=t_s\}$ can be denoted as:

$$\begin{aligned} &Pr\{K=k|T_s=t_s\} \\ &= Pr\{t_e + t_{cr_1} + t_{cr_2} + \cdots + t_{cr_{k-1}} < t_s \leq \\ &\quad t_e + t_{cr_1} + t_{cr_2} + \cdots + t_{cr_k}\} \\ &= \int_{t_e=0}^{\infty}\int_{t_{cr_1}=0}^{\infty}\cdots\int_{t_{cr_k}=0}^{\infty}\int_{t=t_e+t_{cr_1}+\cdots+t_{cr_{k-1}}}^{t_e+t_{cr_1}+\cdots+t_{cr_k}} \\ &f_s(t) f_e(t_e) f_{cr}(t_{cr_1}) f_{cr}(t_{cr_2}) \ldots f_{cr}(t_{cr_k}) dt dt_{cr_k} \ldots dt_{cr_1} dt_e \\ &= \int_{t_e=0}^{\infty}\int_{t_{cr_1}=0}^{\infty}\cdots\int_{t_{cr_k}=0}^{\infty}\int_{t=t_e+t_{cr_1}+\cdots+t_{cr_{k-1}}}^{t_e+t_{cr_1}+\cdots+t_{cr_k}} \\ &\quad \mu_s e^{-\mu_s t} f_e(t_e) \mu_{cr}^k \Big[\prod_{i=1}^{k} e^{-\mu_{cr} t_{cr_i}}\Big] dt dt_{cr_k} \ldots dt_{cr_1} dt_e \\ &= \int_{t_e=0}^{\infty}\int_{t_{cr_1}=0}^{\infty}\cdots\int_{t_{cr_k}=0}^{\infty} e^{-\mu_s(t_e+t_{cr_1}+\cdots+t_{cr_{k-1}})} \\ &\quad (1-e^{-\mu_s t_{cr_k}}) f_e(t_e) \mu_{cr}^k \Big[\prod_{i=1}^{k} e^{-\mu_{cr} t_{cr_i}}\Big] dt_{cr_k} \ldots dt_{cr_1} dt_e \\ &= \Big[\int_{t_e=0}^{\infty} e^{-\mu_s t_e} f_e(t_e) dt_e\Big]\Big[f_{cr}^*(\mu_s)\Big]^{k-1}\Big[1 - f_{cr}^*(\mu_s)\Big] \\ &= f_e^*(\mu_s)\Big(\frac{\mu_{cr}}{\mu_{cr}+\mu_s}\Big)^{k-1}\Big(\frac{\mu_s}{\mu_{cr}+\mu_s}\Big)\,. \end{aligned} \quad (7)$$

Again, according to the *Excess Life Theorem* [29], we have

[5]Generally, a session may be terminated by various reasons. In this study, we mainly focus on the termination because there is no X2 interface.

$f_e(t) = \mu_{cr}\int_{\tau=t}^{\infty} f_{cr}(\tau)d\tau = \mu_{cr}e^{-\mu_{cr}t}$, and the Laplace-Stieltjes transform of $f_e(t)$ is:

$$f_e^*(\mu_s) = \frac{\mu_{cr}}{\mu_{cr}+\mu_s}. \tag{8}$$

From Eq. (8), Eq. (7) is rewritten as:

$$Pr\{K=k|T_s=t_s\} = \frac{\mu_s}{\mu_{cr}+\mu_s}\Big(\frac{\mu_{cr}}{\mu_{cr}+\mu_s}\Big)^k, \text{for } k \geq 1. \tag{9}$$

Next, we discuss the special case $K=0$, i.e., UE finishes the session without performing handover. $Pr\{K=0|T_s=t_s\}$ can be derived as:

$$\begin{aligned} &Pr\{K=0|T_s=t_s\} \\ &\quad = Pr\{t_s < t_e\} \\ &\quad = \int_{t_e=0}^{\infty}\int_{t=0}^{t_e} f_s(t)f_e(t_e)dtdt_e \\ &\quad = 1 - \frac{\mu_{cr}}{\mu_s}\Big[1 - f_{cr}^*(\mu_s)\Big] = \frac{\mu_s}{\mu_{cr}+\mu_s}. \end{aligned} \tag{10}$$

Finally, Eq. (9) and Eq. (10) can be integrated together as:

$$Pr\{K=k|T_s=t_s\} = \frac{\mu_s}{\mu_{cr}+\mu_s}\Big(\frac{\mu_{cr}}{\mu_{cr}+\mu_s}\Big)^k, \text{for } \ k \geq 0. \tag{11}$$

According to Eqs. (6) and (11), Eq. (5) is rewritten as:

$$\begin{aligned} p_c &= \sum_{k=0}^{\infty} Pr\{K=k|T_s=t_s\}\cdot p_s^k \\ &= \frac{\mu_s}{\mu_{cr}+\mu_s}\sum_{k=0}^{\infty} p_s^k\Big(\frac{\mu_{cr}}{\mu_{cr}+\mu_s}\Big)^k \\ &= \frac{\mu_s}{\mu_{cr}+\mu_s}\cdot\frac{1}{1-p_s\Big(\frac{\mu_{cr}}{\mu_{cr}+\mu_s}\Big)} \\ &= \frac{\mu_s}{\mu_s+\mu_{cr}(1-p_{X2})\Big[1-\Big(\frac{k\mu_b}{k\mu_b+\lambda_r}\Big)^k\Big]}. \end{aligned}$$

Thus, the eMBMS session failure probability, p_{nc}, that a UE service session encounters handover failure(s) caused by S1-based handover (without X2 interface) is:

$$p_{nc} = 1 - p_c = \frac{\mu_{cr}(1-p_{X2})\Big[1-\Big(\frac{k\mu_b}{k\mu_b+\lambda_r}\Big)^k\Big]}{\mu_s+\mu_{cr}(1-p_{X2})\Big[1-\Big(\frac{k\mu_b}{k\mu_b+\lambda_r}\Big)^k\Big]}.$$

C. Modeling of Average UE Service Time

The UE service time, T_f, is defined as the time between a UE joining the service and the time the UE forced to be terminated due to handover failures. $E[T_f]$ is its mean value. Increasing $E[T_f]$ increases the probability that UEs in the network can enjoy eMBMS service long enough before encountering a handover failure. For example, if a cellular operator knows that the staying time of its major eMBMS subscribers (say 90%) is less than one hour, the operator may try to improve its network for $E[T_f] \geq 3600$s, which guarantees that 90% users can complete their service session successfully.

Next, we will derive $E[T_f]$. Let K be the number of handovers within the UE's eMBMS session and I be the number that a UE crosses cells between two handover failures. Therefore,

$$T_f = \begin{cases} t_e, & I=1, \\ t_e + t_{cr_1} + \cdots + t_{cr_{I-1}}, & 2 \leq I \leq K. \end{cases}$$

Both the numbers that a UE crosses cells during its session K and the session holding time T_s are independent of the cell residence time. Moreover, t_e, t_{cr_n}, $n \in \{1, \cdots, i-1\}$ are independent of each other. That is,

$$\begin{aligned} &E[t_e + t_{cr_1} + \cdots t_{cr_{i-1}}|I=i] \\ &= E[t_e] + E[t_{cr_1}] + E[t_{cr_2}] + \cdots + E[t_{cr_{i-1}}] \\ &= \int_{t_e=0}^{\infty} t_e f_e(t_e)dt_e + (i-1)\int_{t_{cr}}^{\infty} t_{cr}f_{cr}(t_{cr})dt_{cr} \\ &= \int_{t_e=0}^{\infty} t_e\mu_{cr}e^{-\mu_{cr}t_e}dt_e + (i-1)\int_{t_{cr}}^{\infty} t_{cr}\mu_{cr}e^{-\mu_{cr}t_{cr}}dt_{cr} \\ &= \frac{i}{\mu_{cr}}, \quad 1 \leq i. \end{aligned} \tag{12}$$

Furthermore, $Pr\{I=i\}$ is the probability that a UE encounters the first handover failure at its i^{th} handover. That means previous $i-1$ handovers are all successful. We then can derive $Pr\{I=i\}$ as:

$$Pr\{I=i\} = p_s^{i-1}(1-p_s), \ \ 1 \leq i. \tag{13}$$

According to Eqs. (12) and (13), the average UE service time is derived as:

$$\begin{aligned} E[T_f] &= \sum_{i=1}^{\infty} E[T_f|I=i]Pr\{I=i\} \\ &= \sum_{i=1}^{\infty} E[t_e + t_{cr_1} + \cdots + t_{cr_{i-1}}|I=i]Pr\{I=i\} \\ &= \sum_{i=1}^{\infty} \frac{i}{\mu_{cr}}\cdot p_s^{i-1}(1-p_s) \\ &= \frac{1}{\mu_{cr}\Big[1-\Big(\frac{k\mu_b}{k\mu_b+\lambda_r}\Big)^k\Big](1-p_{X2})}. \end{aligned} \tag{14}$$

D. Modeling of Extra Authentication Loads for UE and CN

Extra authentication load is defined as the authentication load caused by handover failures. When a UE suffers from handover failures due to rekeying, as shown in Fig. 2, the UE needs to conduct User Service Join procedure Step 1 - Step 5, which incur extra signaling cost for both UE and CN. Also, if a UE suffers from three handover failures within its session, the UE needs to conduct authentication procedure three times to complete the session. We use $E[C_{ReAuth\_UE}]$ and $E[C_{ReAuth\_core}]$ to denote the extra authentication loads for UE and CN, respectively. We derive them as follows:

$$\begin{aligned} &E[C_{ReAuth\_UE}] \\ &\quad = \frac{E[T_s]}{E[T_f]} = \frac{\mu_{cr}}{\mu_s}\Big[1-\Big(\frac{k\mu_b}{k\mu_b+\lambda_r}\Big)^k\Big](1-p_{X2}), \end{aligned} \tag{15}$$

and

$$\begin{aligned} &E[C_{ReAuth\_core}] \\ &= E[\text{NO. of UEs in system}]E[C_{ReAuth\_UE} \text{ per second}] \\ &= \lambda_s \cdot \frac{1}{\mu_s} \cdot E[C_{ReAuth\_UE}] \cdot \mu_s \\ &= \frac{\lambda_s \mu_{cr}}{\mu_s}\left[1 - \left(\frac{k\mu_b}{k\mu_b + \lambda_r}\right)^k\right](1 - p_{\text{X2}}). \end{aligned} \tag{16}$$

VII. Numerical Results

The analytical results in Section VI are validated by extensive simulations by using ns-2, version 2.35 [31]. The ns-2 simulator is used to define the motion mode of the UEs, to simulate the handover behaviors using S1 interface and X2 interface, to configure eNBs and UEs, and to create the statistical data track log files. The simulation experiments are generated and simulated on an Intel Core i7 3.9 GHz machine using 8 GB RAM, Ubuntu 12.04 LTS.

Stochastic parameters are involved in the simulations and are summarized in Table 1. If not further specified, the following parameters are set as the default values for performance comparison: $\frac{1}{\mu_s} = 3600$ s, $\frac{1}{\mu_{cr}} = 60$ s, $\frac{1}{\mu_b} = 0.5$ s, $p_{\text{X2}} = 50\%$, and $\lambda_s = 5$ (1/s). Here we show an example in the simulations. During a session holding time t_s, a UE will visit K cells (with cell residence time t_{cr_i} in i^{th} cell). The UE's eMBMS session holding time t_s and cell residence time t_{cr} are assumed to be exponential distributed. With the stochastic parameters t_s and t_{cr_i}, the number of handovers during the UE's session time, K, is different from time to time. Also, the data buffer time at current serving eNB t_b is relaxed as general distribution by considering traffic conditions.

The simulation results are the average over 100,000 simulations. In general, the simulation results fit to the analytical results. Due to the page limit, in the following figures we only show the results with respect to Gamma distribution. Another reason is that the distribution of any positive random variable can be approximated by a combination of Gamma distribution as stated in Lemma 3.9 in [30]. Moreover, in the figures, the *lines* denote analytical results, and the *points* represent simulation results.

A. Impacts of S1 and X2 Interfaces on eMBMS Handover Failure Probability

Fig. 10 and Fig. 11 show the impacts of S1/X2 interface and data buffered time on handover failure probability p_f and p_h. Recall that p_f is the handover failure probability in the network when only S1 interface is deployed, whereas p_h denotes the handover failure probability considering the impacts of X2 interface. The results are compared with $\frac{1}{\mu_b}$, the mean value of data buffered time t_b in the source eNB for different network conditions (i.e., signal strength). We observe that reducing t_b (i.e., improve network condition) has positive impacts on both p_f and p_h. We also observe that the variation of p_f and p_h is not linear and is much slower than the changing of $\frac{1}{\mu_b}$ when we double the value of $\frac{1}{\mu_b}$ from 0.3 s to 0.6 s (or 0.6 s to 1.2 s). Therefore, improving network condition to good signal strength is helpful to both p_f and p_h. However, it may not be cost effective.

Next, we further investigate the impacts of S1 interface and X2 interface on handover failure probability. Fig. 10(A) shows p_f, the handover failure probability using S1 interface, and Fig. 10(B) illustrates p_h, the handover failure probability using X2 interface. It is easy to see that X2-based handover has much lower handover failure probability compared with S1-based handover. Specifically, we compare both p_f and p_h with different UE arrival rate λ_s. Initially, we set λ_s as 1 arrival/s and slowly increased it to 10 arrival/s. We observe that both p_f and p_h increases significantly at the beginning (i.e., λ_s from 1 arrival/s to 5 arrival/s) and increases slightly afterwards. The reason is that increasing rekeying rate may lead to loss of rekeying information in the buffer of the source eNB. When the rekeying operation occurs frequently, the rekeying information are more likely to be in the buffer of the source eNB while a UE hands over to its target eNB. The results validate our analytical models and discussions that reducing λ_s decreases p_f. Moreover, the results of Fig. 10(A) suggest that decreasing λ_s from 10 arrival/s to 5 arrival/s almost does not help to diminish the impacts of S1 interface on p_f. In other words, cellular operators are suggested to decrease λ_s down to be less than 5 arrival/s for the improvement on p_f. The results also give optimization guidelines for our proposed solutions which will be presented in Section VIII. In addition, Fig. 10(B) also shows that p_h is always less than $1-p_{\text{X2}}$, regardless either network condition or UE arrival rate, or both. These suggest cellular operators that adding X2 interface in the network is more efficient than improving network condition on p_h.

Fig. 11 shows the impacts of X2 interface on p_h. The figure indicates that handover failure probability, p_h, can be down to 0% when X2 interfaces are deployed in the whole network. In addition, when we increase the X2 interface probability, the p_h decreases when p_{X2} increases. We also see that when p_{X2} grows from 0% to 50%, the p_f drops by 35.3% and 18.7% with $1/\mu_b = 1.2$ s and $1/\mu_b = 0.3$ s, respectively. This reflects that the existence of X2 interfaces has greater impact than improving network condition. Furthermore, cellular operators are suggested to replace S1 interface with X2 interface in the networks if network condition is poor.

These results suggest cellular operators that adding X2 interface in the network is more efficient than improving network condition on p_h. Furthermore, cellular operators are suggested to replace S1 interface with X2 interface in the networks if network condition is poor.

B. Impacts of S1 and X2 Interfaces on eMBMS Session Failure Probability

Fig. 12 shows the impacts of mean value of session life time $\frac{1}{\mu_s}$, X2 existing probability p_{X2}, mean value of data buffered time $\frac{1}{\mu_b}$, rekeying time interval t_I, and mean value of cell residence time $\frac{1}{\mu_{cr}}$ on session failure probability p_{nc}, respectively. We first take a look at $\frac{1}{\mu_s}$. We can see that large value of $\frac{1}{\mu_s}$ (3600 s) leads to higher p_{nc} than smaller $\frac{1}{\mu_s}$

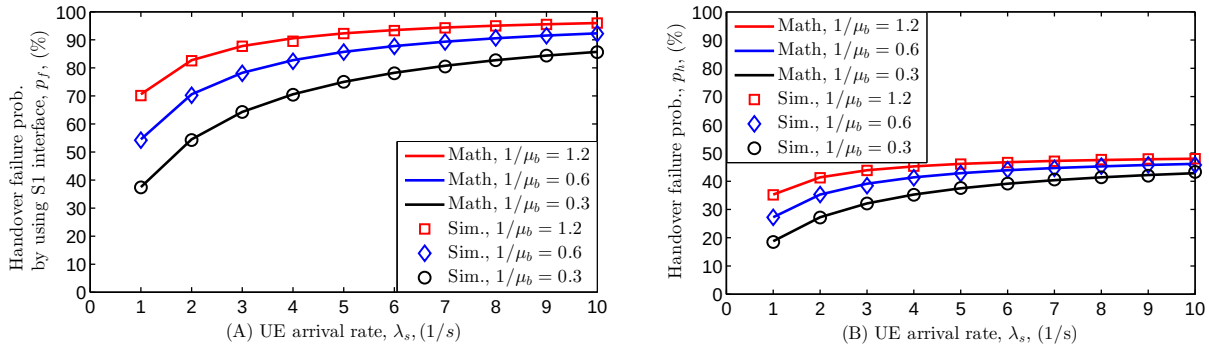

Fig. 10: Handover failure probability of S1-based handover and that of X2-based handover versus UE arrival rate to a specific MBMS user service. Note that the unit of $1/\mu_b$ is second.

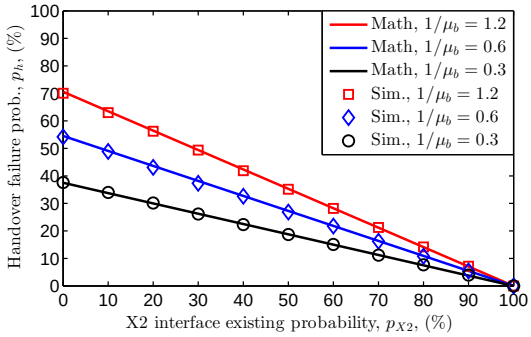

Fig. 11: eMBMS handover failure probability versus existing probability of X2 interface. Note that the unit of $1/\mu_b$ is second.

does. The reason is that long session life time means UEs suffering from more handover failures. Therefore, it results in more session failure. An interesting observation in Figs. 12(C) and 12(D) is that long session life time leads to considerable raise of p_{nc}, if t_I and $\frac{1}{\mu_{cr}}$ are in small values (between 60 s and 180 s). These results indicate that long session life time is very sensitive to t_I and $\frac{1}{\mu_{cr}}$. Therefore, to guarantee users' QoE, cellular operators are suggested to reduce rekeying rate in the areas with high UE mobility and for the eMBMS services with long session life time.

More specifically, Figs. 12(A) and 12(B) illustrate the impact of p_{X2} and $\frac{1}{\mu_b}$ on p_{nc}, respectively. Similar to the results in Fig. 11, increasing X2 interface and improving network condition have positive impacts on p_{nc}. This is due to the fact that less handover failures make the session more likely to be successfully completed. Furthermore, the impacts of t_I and $\frac{1}{\mu_{cr}}$ are shown in Figs. 12(C) and 12(D). We observe that p_{nc} declines significantly when either t_I or $\frac{1}{\mu_{cr}}$ increases from 60 s to 180 s, and then the curves descent slowly afterwards. Based on the results, our suggestions to cellular operators are twofold: (1) Increasing t_I to a suitable value can find a balance point to guarantee both users' QoE and the interest of the content providers. For example, $t_I = 60$ s for $\frac{1}{\mu_s} = 600$ s, or, $t_I = 120$ s for $\frac{1}{\mu_s} = 3600$ s. Large t_I may hurt the interest of the content provider (revenue loss), whereas small one may result in the deterioration of users' QoE. (2) Deploying X2 interface does not make significant improvement on p_{nc} in the areas with low UE mobility (e.g., $\frac{1}{\mu_{cr}} \geq 300$ s). The operators are not suggested to deploy X2 interface in those areas if they care about the deployment cost of X2 interface.

C. Impacts of S1 and X2 Interfaces on Average UE Service Time

In this section, we study the average UE service time, $E[T_f]$, versus X2 interface existing probability, p_{X2}, as shown in Figs. 13(A)-(C). We scale p_{X2} from 0% to 90% and observe that $E[T_f]$ increases exponentially when p_{X2} grows. One interesting observation is that $E[T_f]$ increases very slowly when p_{X2} is less than 40%, but grows significantly after 40%. This tells operators that although adding X2 interface into legacy network inceases $E[T_f]$, deploying X2 interfaces makes nearly no difference to QoE if $p_{\text{X2}} \leq 40\%$.

More specifically, Fig. 13(A) illustrates both the analytical and simulation results of $E[T_f]$ by considering the mean value of cell residence time, $\frac{1}{\mu_{cr}}$, with respect to 60 s, 120 s, and 240 s, respectively. We can see that longer cell residence time results in larger $E[T_f]$. In other words, high mobility UEs are more likely to suffer from handover failure. Therefore, legacy networks serving high mobility UEs are suggested to increase X2 interface probability. For example, the eNBs near freeways are recommended to deploy X2 interface. Fig. 13(B) shows the impacts of data buffered time $\frac{1}{\mu_b}$ on $E[T_f]$. In the simulations, we adjusted $\frac{1}{\mu_b}$ from 0.3 s to 1.2 s. The results show that it has less effects on $E[T_f]$ compared with $\frac{1}{\mu_{cr}}$. Fig. 13(C) depicts that high UE arrival rate λ_s reduces $E[T_f]$ slightly.

In conclusion, in the above parameters, p_{X2} has the most considerable impacts on $E[T_f]$. By adding X2 interface into legacy networks, $E[T_f]$ can be significantly improved. If the deployment cost of X2 interface matters, we suggest operators deploy X2 interface in the area with high mobility UEs (e.g., near freeways, railways) and increase X2 interface to at least 40%.

D. Impacts of S1 and X2 Interfaces on Extra Authentication Load for UE and CN

Figs. 14(A)-(D) illustrate the average number of re-authentication procedures that a UE needs to perform if it wants to complete its eMBMS session. The figure shows that $E[C_{ReAuth\_UE}]$ decreases when p_{X2} increases. That is,

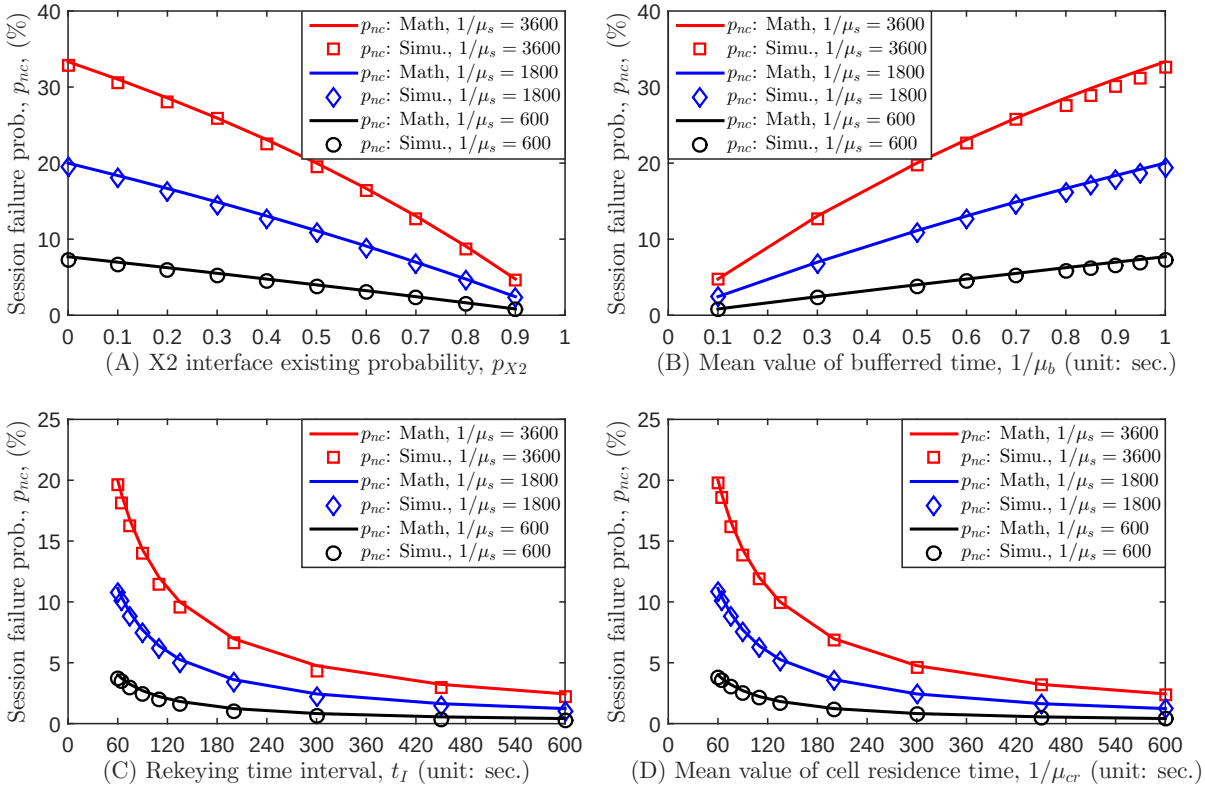

Fig. 12: Session failure probability versus p_{X2}, $\frac{1}{\mu_b}$, t_I, and $\frac{1}{\mu_{cr}}$. Note that the unit of $1/\mu_s$ is second.

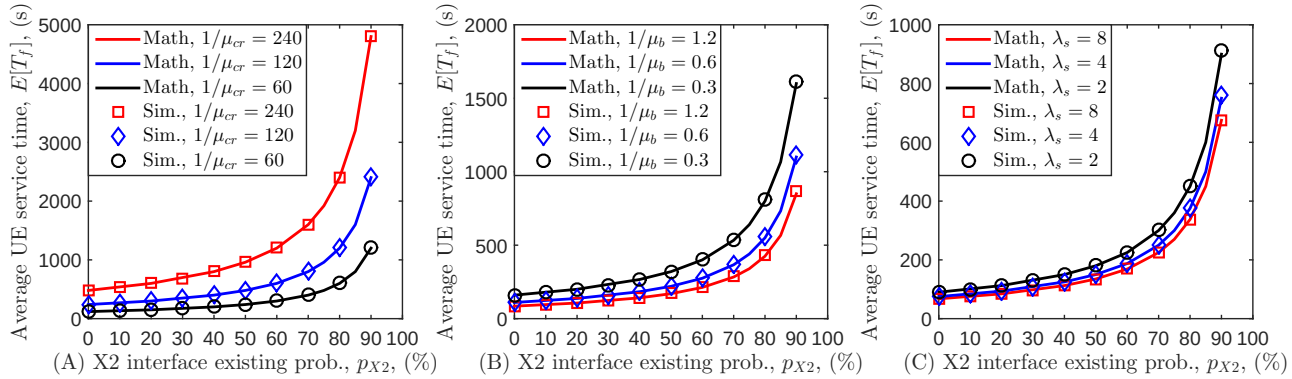

Fig. 13: Average time between two successive handover failures versus existing probability of X2 interface with different $\frac{1}{\mu_{cr}}$, $\frac{1}{\mu_b}$, and λ_s in (A), (B) and (C), respectively. Note that the units of $1/\mu_{cr}$ and $1/\mu_b$ are second. The unit of λ_s is arrival/s.

increasing X2 interfaces does help a UE to reduce its extra authentication load.

In particular, we further investigate the extra authentication load for UE, $E[C_{ReAuth\_UE}]$, by considering average session time in Fig. 14(A), average cell residence in Fig. 14(B), average data buffered time in Fig. 14(C), and UE arrival rate in Fig. 14(D). Figs. 14(A) and 14(B) are similar, where we adjust either $\frac{1}{\mu_s}$ or $\frac{1}{\mu_{cr}}$ by doubling its value from time to time. We observe that the curves of either $\frac{1}{\mu_s}$ or $\frac{1}{\mu_{cr}}$ are linear. Whereas, in Figs. 14(C) and 14(D), we can see that the growths of both $\frac{1}{\mu_b}$ and λ_s only lead to slight gains of $E[C_{ReAuth\_UE}]$. One interesting observation is that the authentication load rises almost 20% by doubling λ_s from 2 (1/s) to 4 (1/s), compared with only 10% gains when λ_s is further doubled from 4 (1/s) to 8 (1/s). This indicates that λ_s has less and less impact on $E[C_{ReAuth\_UE}]$ when it increases. Similar observations are also found for the impacts of data buffered time on $E[C_{ReAuth\_UE}]$, which means that operators only need to keep network condition on a certain level. Also, it will not give much help on reducing $E[C_{ReAuth\_UE}]$ if the network condition already exceeds the level.

Furthermore, Figs. 15(A)-(D) shows the extra authentication load for CN, $E[C_{ReAuth\_core}]$, by considering average session time in Fig. 15(A), average cell residence time in Fig. 15(B), average data buffered time in Fig. 15(C), and UE arrival rate in Fig. 15(D). Similar to Figs. 14(A)-(C), Figs. 15(A)-(C)

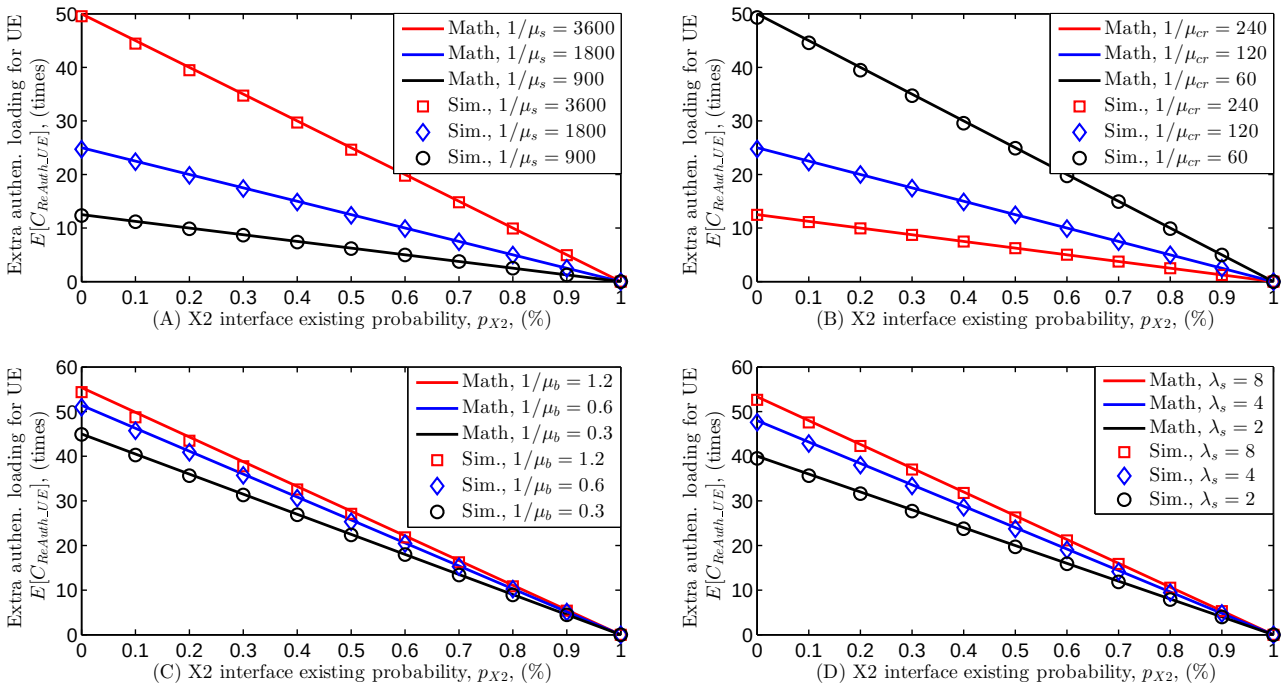

Fig. 14: Extra authentication load for UE versus existing probability of X2 interface with different $\frac{1}{\mu_s}$, $\frac{1}{\mu_{cr}}$, $\frac{1}{\mu_b}$, and λ_s in (A), (B), (C) and (D), respectively. Note that the units of $1/\mu_s$, $1/\mu_{cr}$, and $1/\mu_b$ are second. The unit of λ_s is arrival/s.

also demonstrate that the growth of X2 interface probability diminishes $E[C_{ReAuth\_core}]$ significantly, and that decreasing one of $\frac{1}{\mu_s}$, $\frac{1}{\mu_{cr}}$, or $\frac{1}{\mu_b}$ reduces the authentication overhead for CN. Differing from Fig. 14, the results shown in Fig. 15 illustrate that the increment of λ_s leads to considerable growth of $E[C_{ReAuth\_core}]$. The reason is that the more UEs joining the service, the more UE session failures.

In conclusion, in UE's side, λ_s has less impacts on $E[C_{ReAuth\_UE}]$ because the handover failure probability approaches to $1 - p_{\text{X2}}$ even when λ_s approaches to infinite. However, in CN side, μ_b has less impact. The reason is that the average number of UEs staying in the eMBMS session becomes dominant to the $E[C_{ReAuth\_core}]$.

VIII. Guidelines for Operators

In the above two sections, we provide a systematic way to investigate the handover failure problem in eMBMS. We have derived and discussed five performance metrics: handover failure probability p_h, session failure probability p_{nc}, average UE service time $E[T_f]$, and extra authentication cost ($E[C_{ReAuth\_UE}]$ and $E[C_{ReAuth\_core}]$). Based on them, we conclude that cellular operators can improve the network performance by adjusting any (or all) of the parameters.

In this section, we first use a case study to show that system performance can be significantly improved by changing one of the parameters, where we use rekeying rate as an alternative for X2 in the areas with low UE mobility. Next, evaluation of the proposed solution is discussed, followed by our guidelines for operators.

A. A Solution: Dynamic Rekeying Interval

Considering a scenario that Facebook Live is going to take place, there might be bursty UE arrivals for the eMBMS service. In order to provide forward security in the service, left UEs should be revoked so that they cannot access the eMBMS content encrypted by the new keys. Rekeying operations are performed if a UE joins/leaves the eMBMS service (see Section II-B). In such situation, rekeying rate will increase if bursty UEs arrive, resulting in the surge of missing rekeying information. The performance can be improved if we can reduce rekeying rate.

There are some ways to reduce rekeying rate. In [16], we proposed to prolong rekeying interval dynamically. Although increasing rekeying interval is a straightforward approach to reduce rekeying rate, it is not intuitive when the interests of content providers are taken into consideration. In eMBMS service, the content providers charge for the multimedia content they provide. Prolonging rekeying interval means that left UEs are still able to access eMBMS content, resulting in revenue loss for the content providers. Here comes with the tradeoff between the cellular network operators and the content providers. Interested readers can refer to our recent work in [16]. In this paper, however, we mainly focus on the impacts of prolong rekeying interval dynamically from cellular operators' perspective (i.e., reducing authentication costs for CN and UE).

We denote the prolonged rekeying interval as t_{I_l} and the time interval between the UE hands over to the next eNB and the first rekeying operation occurs as t_{r_l}. Next, to investigate the impact of the prolonged rekeying interval, we model the handover failure probability with t_{r_l} as follows.

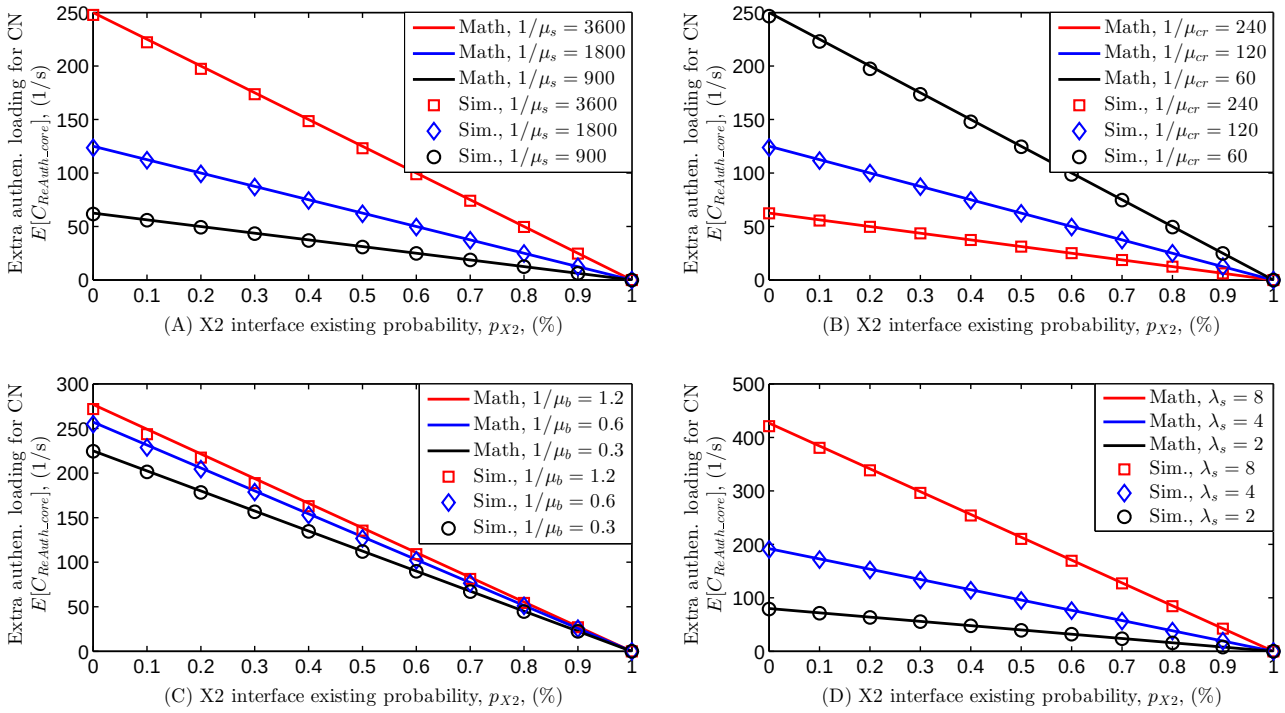

Fig. 15: Extra authentication load for CN versus existing probability of X2 interface with different $\frac{1}{\mu_s}$, $\frac{1}{\mu_{cr}}$, $\frac{1}{\mu_b}$, and λ_s in (A), (B), (C) and (D), respectively. Note that the units of $1/\mu_s$, $1/\mu_{cr}$, and $1/\mu_b$ are second. The unit of λ_s is arrival/s.

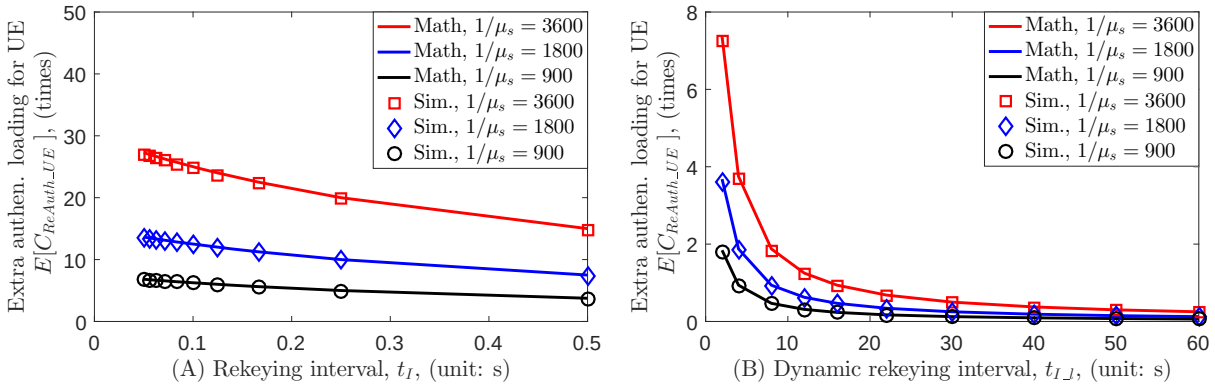

Fig. 16: Impacts of prolonging rekeying time interval on extra authentication load for UE. Note that the unit of $1/\mu_s$ is second.

The probability that rekeying information is not included in the buffered data of the serving eNB when the UE hands over to its target eNB is:

$$\begin{aligned} &Pr\{t_b \le t_{r\_l}\} \\ &= \int_{-\infty}^{\infty} Pr\{t_b \le t_{r\_l} | t_{r\_l} = t\} f_{r\_l}(t) dt \\ &= \int_{t=0}^{t_{I\_l}} Pr\{t_b \le t | t_{r\_l} = t\} f_{r\_l}(t) dt \\ &\quad (\text{since } 0 \le t_{r\_l} < t_{I\_l}) \\ &= \int_{t=0}^{t_{I\_l}} \int_{t_b=0}^{t} f_b(t_b) f_{r\_l}(t) dt_b dt, \end{aligned} \tag{17}$$

where $f_{r\_l}(t)$ is the pdf of t_{r_l}.

As aforementioned discussion, the rekeying interval becomes deterministically distributed in steady state with the rekeying rate $\frac{1}{t_{I\_l}}$. According to the *Excess Life Theorem* [29], we have:

$$f_{r\_l}(t) = \frac{1}{t_{I\_l}} \int_{s=t}^{\infty} f_{I\_l}(s) ds = \frac{1}{t_{I\_l}} \Big[1 - F_{I\_l}(t)\Big]. \tag{18}$$

The rekeying operation has a pmf (probability mass function) given by: $p_{I\_l}(m) = \frac{t_{I\_l}}{t_s}$, $m \in \mathbb{N}^0, m \in \Big[0, \Big\lfloor \frac{t_s}{t_{I\_l}} \Big\rfloor\Big)$. Its CDF is then given as:

$$F_{I\_l}(t) = \begin{cases} \frac{m}{t_s} t_{I\_l}, & m t_{I\_l} \le t < (m+1) t_{I\_l}; \\ 1, & \Big\lfloor \frac{t_s}{t_{I\_l}} \Big\rfloor t_{I\_l} \le t < t_s; \end{cases} \tag{19}$$

where $m \in \mathbb{N}^0$, $m \in \Big[0, \Big\lfloor \frac{t_s}{t_{I\_l}} \Big\rfloor\Big)$. Therefore, from

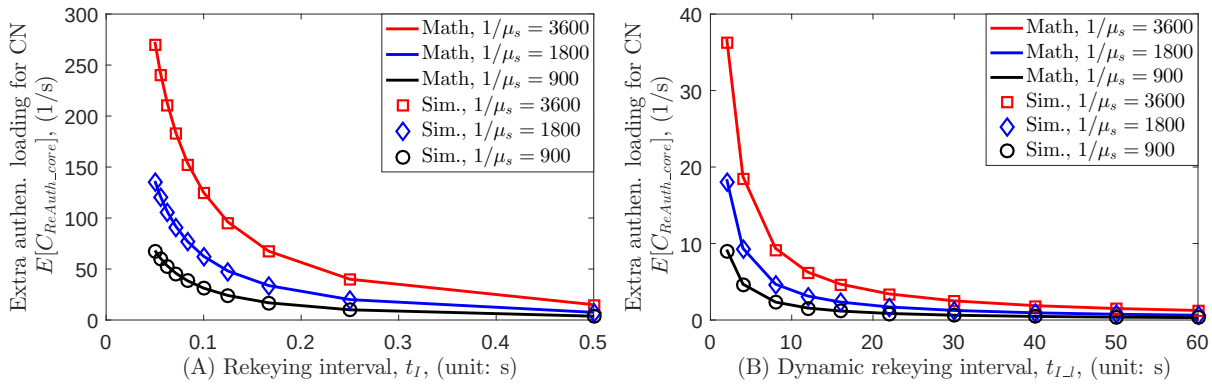

Fig. 17: Impacts of prolonging rekeying time interval on extra authentication load for CN. Note that the unit of $1/\mu_s$ is second.

Eqs. (18) and (19), Eq. (17) is rewritten as:

$$\begin{aligned}
&Pr\{t_b \le t_{r_l}\} \\
&= \int_{t=0}^{t_{I_l}} \int_{t_b=0}^{t} f_b(t_b)\frac{1}{t_{I_l}}\Big[1 - F_{I_l}(t)\Big]dt_b dt \\
&= \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} \int_{t=t_b}^{t_{I_l}} f_b(t_b)\Big[1 - F_{I_l}(t)\Big]dt dt_b \\
&= \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} \int_{t=t_b}^{t_{I_l}} f_b(t_b) dt dt_b \\
&\quad \Big(\text{by } F_{I_l}(t) = 0, \text{ if } 0 \le t < t_{I_l}\Big) \\
&= \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} f_b(t_b)(t_{I_l} - t_b)dt_b \\
&= \int_{t_b=0}^{t_{I_l}} f_b(t_b)dt_b - \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} f_b(t_b)t_b dt_b \\
&= F_b(t_{I_l}) - F_b(t_{I_l}) + \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} F_b(t_b)dt_b \\
&= \frac{1}{t_{I_l}} \int_{t_b=0}^{t_{I_l}} F_b(t_b)dt_b. \qquad (20)
\end{aligned}$$

Hence, Eq. (2) is then rewritten as:

$$p_{f\_l} = 1 - \frac{1}{t_{I\_l}} \int_{t_b=0}^{t_{I\_l}} F_b(t_b)dt_b. \qquad (21)$$

In the following, p_{f_l} is shown based on the distribution of buffered data time, t_b, with Gamma distribution, Erlang distribution, and exponential distribution, respectively.

Gamma Distribution: The CDF of Gamma distribution, Gamma$(k, \frac{1}{k\mu_b})$, is $F_b(t_b) = \frac{1}{\Gamma(k)}\gamma(k, k\mu_b t_b)$. Hence, Eq. (21) is rewritten as: $p_{f\_l} = 1 - \frac{1}{t_{I\_l}} \int_{t_b=0}^{t_{I\_l}} \frac{1}{\Gamma(k)}\gamma(k, k\mu_b t_b)dt_b$.

Erlang Distribution: The CDF of Erlang distribution, Erlang(k, μ_b), is $F_b(t_b) = 1 - \sum_{n=0}^{k-1} \frac{1}{n!} e^{-\mu_b t_b}(\mu_b t_b)^n$. Hence, Eq. (21) is rewritten as: $p_{f\_l} = \frac{1}{t_{I\_l}} \int_{t_b=0}^{t_{I\_l}} \sum_{n=0}^{k-1} \frac{1}{n!} e^{-\mu_b t_b}(\mu_b t_b)^n dt_b$.

Exponential Distribution: The CDF of Exponential distribution, Exp(μ_b), is $F_b(t_b) = 1 - e^{-\mu_b t_b}$. Hence, Eq. (21) is rewritten as: $p_{f\_l} = \frac{1 - e^{-\mu_b t_{I\_l}}}{\mu_b t_{I\_l}}$.

B. Evaluation of the Proposed Solution

As aforementioned discussion, if operators cannot deploy X2 interface due to various reasons, we still can deal with the bursty UE arrivals by adjusting rekeying rate. Accordingly, a solution is proposed. Figs. 16(A)-(B) and Figs. 17(A)-(B) show the simulation and analytical results of the solution on UE and CN, respectively. In the figures, the results with and without our proposed dynamic rekeying are shown in (A) and (B), respectively. We can see that the extra authentication costs of both UE and CN decline significantly. We also observe that in Fig. 16(B) and Fig. 17(B), the extra authentication costs initially drop sharply and then start to descent smoothly. Because a long rekeying interval results in revenue loss for content providers [16], mobile operators can choose appropriate rekeying intervals to alleviate authentication load for both UE and CN based on their closed-forms derived in Eqs. (15), (16).

C. Guidelines

Here, we offer general guidelines for operators. Operators can obtain specific settings by using our analytical models in Section VI.

1) X2 interface existing probability p_{X2}: It is not necessary to deploy X2 interface in the whole network. Operators can only replace S1 interface with X2 interface in part of their networks.
2) Data buffered time t_b in a serving eNB: The data buffered time is closely related to network condition. Generally, good signal strength leads to less data buffered in the serving eNB. The operators can improve their network condition to guarantee good signal strength to reduce t_b.
3) Rekeying rate λ_r: Compared with the above two parameters which are costly and time consuming to improve, the rekeying rate λ_r is the only parameter that the operators can adjust in real time to improve performance.

Due to cost concerns, we suggest that cellular operators deploy X2 interface and improve network condition in the areas in which UEs have short cell residence time t_{cr} (i.e., UEs with high moving speed). In those areas, such as high-speed

railways, freeways, highways, UEs may need to handover from one eNB to another frequently. Either deploying X2 interface or improving signal strength can reduce handover failure probability significantly. In other areas (i.e., networks are not fully deployed with X2 interface), adjusting rekeying rate is a flexible approach to handle bursty UE arrivals.

IX. Summary

In this paper, we identify a new eMBMS handover failure problem caused by KMM when there is only S1 interface available in eMBMS. We then propose comprehensive analytical models to investigate the problem. We model five performance metrics to study the network performance, i.e., eMBMS handover failure probability, eMBMS session failure probability, average UE service time, extra authentication loads for UE, and extra authentication loads for CN. Our analytical models reveal the common properties of the handover failure in eMBMS and its relation to network performance. Furthermore, based on the analytical models and simulation results, we conclude that the existing probability of X2 interface, data buffered time in the serving eNB, and rekeying rate can be adjusted to diminish the impacts of the handover failure. Accordingly, we propose a solution to handle bursty UE arrivals. Both the simulation and analytical results demonstrate that the impacts of the eMBMS handover failure are reduced significantly.

In this paper, we present a systematic way to investigate the handover failure problem in eMBMS. We also provide theoretical guidelines for operators to design and optimize their networks. In order to reduce deployment cost, we suggest operators deploy X2 interface and improve network condition in the areas in which UEs have short cell residence time (i.e., UEs with high moving speed). For the other areas, we suggest adjusting rekeying rate as a flexible approach to handle bursty UE arrivals. The impacts of rekeying rate can be found in our recent work [16].

Acknowledgement

The authors are very grateful for the constructive comments from the anonymous reviewers that improved the quality of the paper significantly. This work was supported in part by the Ministry of Science and Technology of Taiwan under grant numbers MOST 105-2221-E-009-101-MY3, 106-2221-E-009-046-MY3, 106-2221-E-009-047-MY3, 106-2218-E-009-016.

References

[1] STATS. (2016) Sports streaming: Analyzing Super Bowl 50. [Online]. Available: http://www.stats.com/industry-analysis-articles/sports-streaming-analyzing-super-bowl-50/

[2] 3GPP TS 23.246 V14.1.0, *Multimedia Broadcast/Multicast Service (MBMS); architecture and functional description (Release 14)*, Std., Dec. 2016.

[3] GSA, *Evolution to LTE report*, Jul. 2016.

[4] 3GPP TS 25.346 V14.0.0, *Introduction of the Multimedia Broadcast/Multicast Service (MBMS) in the Radio Access Network (RAN); (Release 14)* , Std., Mar. 2017.

[5] 3GPP TS 33.246 V14.0.0, *3G security; security of Multimedia Broadcast/Multicast Service (MBMS) (Release 14)*, Std., Dec. 2016.

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

[7] D. Xenakis, N. Passas, L. Merakos, and C. Verikoukis, "Mobility management for femtocells in LTE-advanced: Key aspects and survey of handover decision algorithms," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 64–91, 2014.

[8] C. H. M. De Lima, M. Bennis, and M. Latva-Aho, "Modeling and analysis of handover failure probability in small cell networks," in *Proc. IEEE INFOCOM Work.*, 2014, pp. 736–741.

[9] Y. Hong, X. Xu, M. Tao, J. Li, and T. Svensson, "Cross-tier handover analyses in small cell networks: A stochastic geometry approach," in *Proc. IEEE ICC*, 2015, pp. 3429–3434.

[10] R. Balakrishnan and I. Akyildiz, "Local anchor schemes for seamless and low-cost handover in coordinated small cells," *IEEE Trans. Mob. Comput.*, vol. 15, no. 5, pp. 1182–1196, 2016.

[11] S. M. Oh, S. Y. Kang, K. C. Go, J. H. Kim, and A. S. Park, "An enhanced handover scheme to provide the robust and efficient inter-beam mobility," *IEEE Commun. Lett.*, vol. 19, no. 5, pp. 739–742, 2015.

[12] Y. B. Lin, S. N. Yang, and C. T. Wu, "Improving handover and drop-off performance on high-speed trains with multi-RAT," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 6, pp. 2720–2725, 2014.

[13] M. S. Pan, T. M. Lin, and W. T. Chen, "An enhanced handover scheme for mobile relays in LTE-A high-speed rail networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 743–756, 2015.

[14] X. Yu, Y. Luo, and X. Chen, "An optimized seamless dual-link handover scheme for high-speed rail," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, p. 1, 2015.

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

[16] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, "Design and analysis of the Key Management Mechanism (KMM) in evolved Multimedia Broadcast/Multicast Service (eMBMS)," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463–8476, Dec. 2016.

[17] Alcatel Lucent, *Backhaul considerations for LTE and LTE-Advanced*, Aug. 2013.

[18] SMEC, *SMEC white paper: LTE femto gateway with X2 broker*, Mar. 2016.

[19] P. Lescuyer and T. Lucidarme, *Evolved Packet System (EPS): The LTE and SAE Evolution of 3G UMTS*. John Wiley & Sons, Ltd, 2008.

[20] 3GPP TS 22.146 V14.0.0 , *Multimedia Broadcast/Multicast Service (MBMS); (Release 14)*, Std., Mar. 2017.

[21] 3GPP TS 23.401 V14.3.0, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 14)* , Std., Mar. 2017.

[22] 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, 2008.

[23] J. Arkko, E. Carrara, F. Lindholm, K. Norrman, and M. Naslund, *MIKEY: multimedia internet keying*, Aug. 2004, RFC 3830.

[24] 3GPP TS 36.300 V14.2.0, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); overall description; (Release 14)*, Std., Apr. 2017.

[25] C. P. Lee and P. Lin, "Modeling delay timer algorithm for handover reduction in heterogeneous radio access networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1144–1156, Feb. 2017.

[26] K.-H. Chen and J.-C. Chen, "Handoff failure analysis of Adaptive Keep-alive Interval (AKI) in 3GPP Generic Access Network (GAN)," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 4226–4237, 2011.

[27] Y.-B. Lin, "Reducing location update cost in a PCS network," *IEEE/ACM Trans. Netw.*, vol. 5, no. 1, pp. 25–33, 1997.

[28] Y.-B. Lin, S. Mohan, and A. Noerpel, "Queueing priority channel assignment strategies for PCS hand-off and initial access," *IEEE Trans. Veh. Technol.*, vol. 43, no. 3, pp. 704–712, 1994.

[29] S. M. Ross, *Introduction to probability models*, 10th ed. Academic press, 2009.

[30] F. P. Kelly, *Reversibility and stochastic networks*. John Wiley & Sons Ltd, 1979.

[31] "The network simulator - ns-2." Available: http://www.isi.edu/nsnam/ns/.

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 was with the Department of Computer Science, National Chiao Tung University (NCTU), Hsinchu, Taiwan, as a Postdoctoral Fellow, an Assistant Research Fellow, and an Adjunct Assistant Professor from 2012 to 2017. He is currently a Lecturer in the School of Computing Science at University of East Anglia (UEA), Norwich, U.K. His current research interests include Internet of Things (IoT) and 5G Mobile Technology: security, performance analysis, protocol design, radio resource allocation, mobile edge computing, WiFi & Bluetooth Technology, 3GPP, LTE, Software Defined Networking (SDN), Network Function Virtualization (NFV), etc. He received the Best Paper Award in 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 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 (NTHU), Hsinchu, Taiwan, as an Assistant Professor, an Associate Professor, and a Full Professor from 2001 to 2008. He was also the Director of the Institute of Network Engineering with National Chiao Tung University (NCTU), Hsinchu, from 2011 to 2014. He has been a Faculty Member with NCTU since 2010. He is currently a Distinguished Professor with the Department of Computer Science, NCTU.

Dr. Chen received numerous awards, including the Outstanding I.T. Elite Award, Taiwan, the Outstanding Teaching Award from College of Computer Science, NCTU, 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. He is a Distinguished Member of the Association for Computing Machinery (ACM). He was a member of the Fellows Evaluation Committee, IEEE Computer Society.

Jui-Chih Chin received his M.S. degree from the Department of Computer Science, National Chiao Tung University (NCTU), Hsinchu, Taiwan, in 2014. He was a senior LTE modem software engineer in MediaTek Inc., Hsinchu, Taiwan. His research interests include mobility management, admission control, resource management, and performance analysis of wireless networks.