How to Reduce Unexpected eMBMS Session Disconnection: Design and Performance Analysis

Tsung-Yen Chan, Yi Ren, Yu-Chee Tseng, *Fellow, IEEE,* and Jyh-Cheng Chen, *Fellow, IEEE*

***Abstract*—In 3GPP eMBMS, sometimes sessions will be disconnected unexpectedly due to the miss of session keys. Although rekeying can prevent old users from getting multicast data, it also causes authorized users to miss subsequent data if they miss the key update messages. Thus, re-authentication is needed to obtain lost keys from KMM. We point out this problem in our previous work [1]. In this paper, we further propose a new KeySet algorithm, which can pre-issue a number of keys to users when they join eMBMS. The advantage is that a user can still decode multicast data even if it misses some key updates tentatively. However, the cost is that allowing some old users to freely enjoying multicast for some time. In this paper, we quantify the tradeoff and derive the optimal case.**

***Index Terms*—LTE broadcast, Multimedia broadcast and multicast service (MBMS), performance analysis, Quality of Experience (QoE).**

I. Introduction

THE explosion of mobile data is fueling the growth of 4G deployment and new services. According to [2], 68% US respondents and 30% users in France indicated intension in watching TV via hand-held devices while on move. To meet the increasing demand for mobile video services, 3GPP proposes the evolved Multimedia Broadcast/Multicast Service (eMBMS) in LTE-A.

Wireless broadcast services are, however, vulnerable to various security attacks since eavesdropping becomes easier. 3GPP introduces Key Management Mechanism (KMM) to protect eMBMS contents. Multimedia contents for the same group of User Equipment (UE) devices can be encrypted by a group key. This implies that when a UE joins/leaves the group, the current key needs to be revoked, referring as *rekeying*. Consequently, a UE holding the old key is unable to access the subsequent content. On the other hand, if a UE experiences tentative disconnection during key update, KMM needs to resend it, referring as *re-authentication*.

Previous studies (e.g., [3]–[7]) have addressed the security-performance tradeoff in wireless networks. A review of key management can be found in [1]. Different from other wireless networks, eMBMS exhibits the following characteristics: (i) massive group numbers, (ii) dynamic group topology, and (iii) unexpected wireless disconnections. These characteristics make re-authentication more frequently. However, the previous researches did not point out the *re-authentication* problem since the unintended disconnection happens unpredictably. We formulate this problem into an analytical model to investigate it. *How to update group keys at a reasonable cost while preventing old users from accessing multicast data poses a challenge*.

Tsung-Yen Chan, Yu-Chee Tseng, and Jyh-Cheng Chen are with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. E-mail: {tychan, yctseng, jcc}@cs.nctu.edu.tw

Yi Ren is with the School of Computing Science, University of East Anglia, Norwich, U.K. E-mail: Edwin.Ren@uea.ac.uk

In this paper, we propose a new KeySet scheme to reduce re-authentication cost while keeping the cost of missing keys low. In our scheme, when a UE joins an eMBMS group, it is pre-assigned a sequence of K keys, instead of one. The first key is the new group key due to the joining of this UE, while the other $K-1$ keys are to be used in the next $K-1$ revoking events. This design greatly relieves the missing key problem. However, a too large K will allow too much free enjoying time. *We will quantify the tradeoff and derive the optimal K later*.

II. Backgrounds

The eMBMS KMM architecture defined in 3GPP consists of Bootstrapping Server Function (BSF), Broads-cast/Multicast Service Center (BM-SC), content provider, Home Subscriber Server (HSS), and UEs. BSF is for initialization when a UE enters an eMBMS system for the first time. BM-SC conducts authentication procedures with UEs. Content provider provides video data. HSS is responsible for user identification.

To protect multicast data, BM-SC generates four security keys, namely eMBMS Request Key (MRK), eMBMS Service Key (MSK), eMBMS Traffic Key (MTK), and eMBMS User Key (MUK). MRK is to authenticate a UE when performing key requests to BM-SC. MUK protects MSK distribution. MSK is to protect the distribution of MTK, while MTK secures multicast data. Fig. 1 illustrates the key relationship, where $A \rightarrow B$ stands for "A *protects* B".

When a UE joins an eMBMS service, the *User Service Join* procedure in Fig. 2 is triggered. $\{X\}_Y$ denotes that key X is encrypted by key Y. $UE_{\{i...j\}}$ refers to the set $\{UE_i, UE_{i+1}, ..., UE_j\}$. In this example, UE_9 is a newly joining one.

- Step 1: UE_9 and BM-SC perform bootstrapping procedure to generate MRK_9 and MUK_9. Then, UE_9 performs the eMBMS *User Service Registration* procedure with BM-SC by using MRK_9.
- Step 2: BM-SC returns HTTP 200 OK Authentication to accept the joining request of UE_9. Otherwise, it returns HTTP 401 WWW-Authentication for rejection.
- Step 3: BM-SC generates the new MSK (MSK_{789}).
- Step 4: BM-SC unicasts the new key MSK_{789} encrypted by MUK_i to $UE_{\{7...9\}}$. Afterward, $UE_{\{7...9\}}$ uses MUK_i to decrypt $\{MSK_{789}\}_{MUK_i}$.
- Step 5: BM-SC generates the new MTK_{1-9}.
- Step 6: In 6(a) and 6(b), BM-SC sends $\{MTK_{1-9}\}_{MSK_{789}}$ to $UE_{\{7...9\}}$. Upon receiving $\{MTK_{1-9}\}_{MSK_{789}}$, $UE_{\{7...9\}}$ decrypts it to get the new MTK_{1-9} by MSK_{789}. Similarly, MTK_{1-9} is encrypted to $UE_{\{1...3\}}$ and $UE_{\{4...6\}}$.
- Step 7: BM-SC continues to broadcast videos encrypted by MTK_{1-9} to $UE_{\{1...9\}}$.

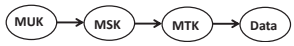


Fig. 1: Key relationship in KMM.

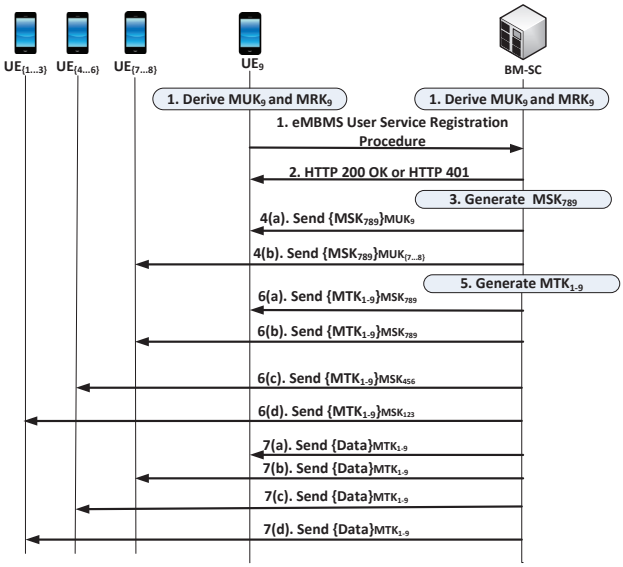


Fig. 2: Example of UE_9 joining an eMBMS service.

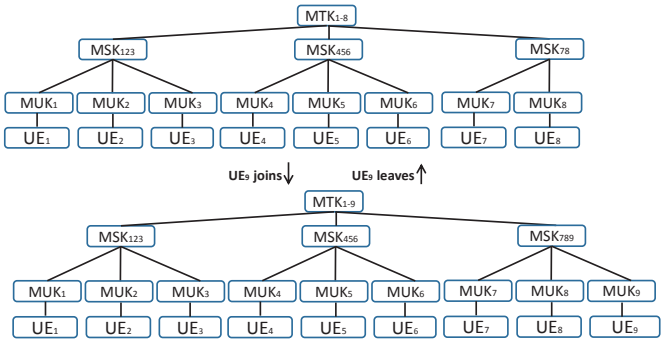


Fig. 3: Key hierarchy in eMBMS.

The leaving procedure is similar and can be found in [8]. Fig. 3 shows the change of key hierarchy when UE joins/leaves the service.

III. Proposed KeySet

In a wireless network, a UE may experience unexpected disconnection. This may lead to a lot of re-authentications as there are more users joining/leaving multicast services. The cost to the core network is thus high. To relieve this problem, we propose a KeySet scheme. Upon entering into eMBMS, a UE will be pre-issued a set of keys $\{\text{MTK}_C, \text{MTK}_{C+1}, \ldots, \text{MTK}_{C+K-1}\}$ from BM-SC, where MTK_C is the current key and the other keys are to be used in the next $K-1$ rounds. Therefore, when a UE experiences temporary disconnection, it has a high chance to decrypt the subsequent content without needing re-authentication. For the core network, whenever the system advances to a new key, it only updates it to those UEs whose latest key has expired. Therefore, the update cost for the core network is also significantly reduced.

One issue is how to choose a suitable K. A larger K leads to less re-authentication cost. However, a larger K also allows old UEs to use their remaining keys to freely enjoy the subsequent contents for a while.

IV. Analysis

In this section, we derive a mathematical model to study the impacts of K. Let $E[C_1]$ be the re-authentication count of a single UE on the original KMM and $E[C_K]$ be that of KeySet. We quantify the performance by the expected re-authentication ratio $\gamma(K) = \frac{E[C_K]}{E[C_1]}$.

Let $E[\text{Free}_K]$ be the potential free enjoying time that a single UE can gain in KeySet.

Below, we introduce some notations (refer to Fig. 4).

1) As that in [1], [9], UEs arrive to an eMBMS service by Poisson process. We have pmf $P(N_A(t) = n) = e^{-\lambda_A t}\frac{(\lambda_A t)^n}{n!}$, where λ_A is the arrival rate and n is the number of arrivals within time t. The problem is modeled as an $M/G/\infty$ system, where departure process is also the same as the arrival process with pmf $P(N_D(t) = n) = e^{-\lambda_D t}\frac{(\lambda_D t)^n}{n!}$, where λ_D=λ_A.
2) The number of rekeying operations in an eMBMS service within t is modeled by $N_R(t)$, which consists the UEs joining and leaving the group, i.e., $N_R(t)$=$N_A(t)$+$N_D(t)$. Since $N_A(t)$ and $N_D(t)$ are i.i.d., we have:

$$\begin{aligned} &P(N_R(t) = n) \\ &= \sum_{k=0}^{n} P(N_A(t) = k)P(N_D(t) = n-k) \\ &= \sum_{k=0}^{n} \left[e^{-\lambda_A t}\frac{(\lambda_A t)^k}{k!}\right] \times \left[e^{-\lambda_D t}\frac{(\lambda_D t)^{n-k}}{(n-k)!}\right] \\ &= e^{-\lambda_R t}\frac{(\lambda_R t)^n}{n!}, \end{aligned}$$

in which $N_R(t)$ is also a Poisson process with rate $\lambda_R = 2\lambda_A$. The pdf of t_R is $f_{t_R}(x) = \lambda_R e^{-\lambda_R x}$, with mean $= \frac{1}{\lambda_R}$. The CDF of t_R is $F_{t_R}(x) = 1 - e^{-\lambda_R x}$.
3) Let t_d be the duration between two disconnections of a single UE. Assume that the arrival of disconnections is a Poisson process with rate λ_d with pmf $P(N_d(t) = n) = e^{-\lambda_d t}\frac{(\lambda_d t)^n}{n!}$. The length of a UE's eMBMS session is modeled by variance t_u with pdf $f_{t_u}(x) = \lambda_u e^{-\lambda_u x}$.
4) Let T_K denote the effective period given a new UE K keys. Since rekeying follows Poisson process, T_K is the sum of K independent exponential random variables. By convolution, T_K is Erlan-distributed with parameter (K, λ_R), pdf $f_{T_K}(x) = \lambda_R e^{-\lambda_R x}\frac{(\lambda_R x)^{K-1}}{(K-1)!}$ and CDF $F_{T_K}(x) = 1 - \sum_{k=0}^{K-1}\frac{1}{k!}e^{-\lambda_R x}(\lambda_R x)^k$. Let t'_R denote the time interval from a UE entering the disconnected status to the next rekeying operation. According to Excess Life Theorem, we have $f_{t'_R}(x) = \frac{1-F_{t_R}(x)}{E[t_R]} = \lambda_R e^{-\lambda_R x}$. Let T'_K denote the time interval from the last time when a UE entering the disconnected status in T_K to the $(C+K)$-th rekeying operation. Again, we have $f_{T'_K}(x) = \frac{\lambda_R}{K}[1 - F_{T_K}(x)] = \frac{\lambda_R}{K}(\sum_{k=0}^{K-1}\frac{1}{k!}e^{-\lambda_R x}(\lambda_R x)^k)$. Let t'_d denote the time duration between a UE entering the disconnected status to its returning to eMBMS. The pdf is $f_{t'_d}(x)$.

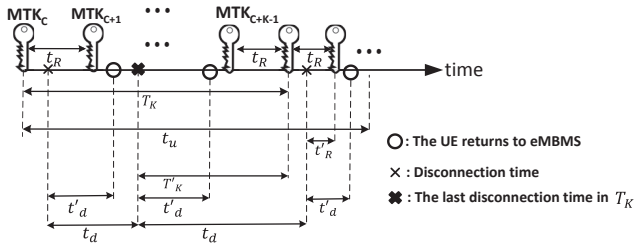


Fig. 4: Illustration of notations.

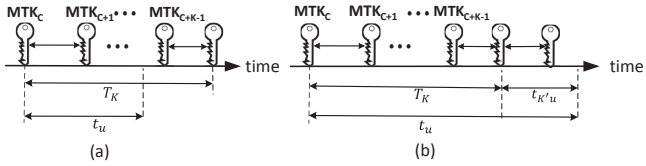


Fig. 5: (a) Case A1: $t_u < T_K$, (b) Case A2: $t_u \geq T_K$.

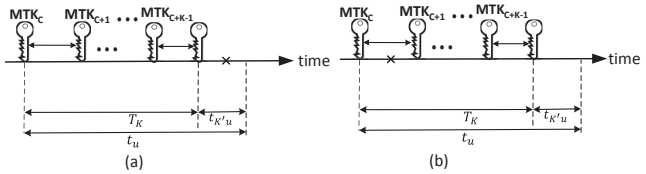


Fig. 6: (a) Case A2a: the first disconnection arrives in $t_{K'u}$, (b) Case A2b: the first disconnection arrives in T_K.

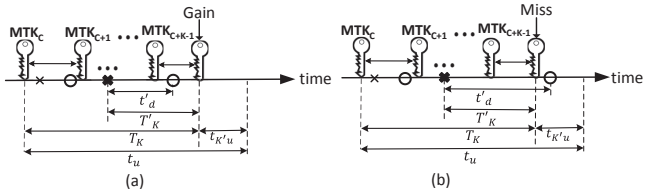


Fig. 7: (a) Case A2b and Case A2b1: $t_u \geq T_K$ and $t'_d < T'_K$, (b) Case A2b and Case A2b2: $t_u \geq T_K$ and $t'_d \geq T'_K$.

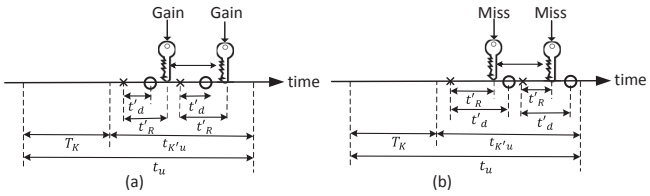


Fig. 8: (a) Case A2 and Case A2c: $t_u \geq T_K$ and $t'_d < t'_R$, (b) Case A2 and Case A2d: $t_u \geq T_K$ and $t'_d \geq t'_R$.

A. Expected Re-authentication Count $E[C_K]$

To derive $E[C_K]$, we consider two cases as shown in Fig. 5. Case A1 is for $t_u < T_K$ and Case A2 is for $t_u \geq T_K$. By total probability formula,

$$E[C_K] = E[C_K|\text{A1}]\ P(\text{A1}) + E[C_K|\text{A2}]\ P(\text{A2}). \quad (1)$$

Case A1: The UE dose not need to perform re-authentication since its remaining keys can be used as shown in Fig. 5(a). So

$$E[C_K|\text{A1}] = E[C_K|t_u < T_K] = 0. \quad (2)$$

Case A2: The re-authentication count is equal to the sum of re-authentication counts in T_K and $t_{K'u}$ as shown in Fig. 5(b). We have

$$E[C_K|\text{A2}] = E[C_{T_K}|\text{A2}] + E[C_{t_{K'u}}|\text{A2}], \quad (3)$$

where $E[C_{T_K}|\text{A2}]$ and $E[C_{t_{K'u}}|\text{A2}]$ are the re-authentication counts in T_K and $t_{K'u}$, respectively. To derive $E[C_{T_K}|\text{A2}]$, we consider two subcases as shown in Fig. 6. Case A2a and Case A2b are for the first disconnection in $t_{K'u}$ and in T_K, respectively. Then, Case A2b1 is for $t'_d < T'_K$ and Case A2b2 is for $t'_d \geq T'_K$ (Fig. 7). To derive $E[C_{t_{K'u}}|\text{A2}]$, we consider two subcases. Case A2c is for $t'_d < t'_R$ and Case A2d is for $t'_d \geq t'_R$ (Fig. 8). We then have:

$$\begin{aligned} E[C_{T_K}|\text{A2}] &= E[C_{T_K}|\text{A2, A2a}]\ P(\text{A2a}) \\ &\quad + E[C_{T_K}|\text{A2, A2b}]\ P(\text{A2b}) \\ &= E[C_{T_K}|\text{A2, A2a}]\ P(\text{A2a}) \\ &\quad + \Big[E[C_{T_K}|\text{A2, A2b, A2b1}]\ P(\text{A2b1}) \\ &\quad + E[C_{T_K}|\text{A2, A2a, A2b2}]\ P(\text{A2b2})\Big] P(\text{A2b}) \quad (4) \end{aligned}$$

$$\begin{aligned} E[C_{t_{K'u}}|\text{A2}] &= E[C_{t_{K'u}}|\text{A2, A2c}]\ P(\text{A2c}) \\ &\quad + E[C_{t_{K'u}}|\text{A2, A2d}]\ P(\text{A2d}). \quad (5) \end{aligned}$$

Case A2a: Since there is no disconnection in T_K, re-authentication is not needed. Thus, $E[C_{T_K}|\text{A2, A2a}] = 0$.

Case A2b: This case may require re-authentication since the first disconnection arrives in T_K. However, we need to consider Case A2b1 and Case A2b2.

Case A2b1: Since the UE returns to eMBMS before the expiration of its K-th key, re-authentication is not needed. Therefore, $E[C_{T_K}|\text{A2, A2b, A2b1}] = 0$.

Case A2b2: In this case, re-authentication is needed because the UE will always miss the $(C+K)$-th rekeying operation. Then, $E[C_{T_K}|\text{A2, A2b, A2b2}] = 1$, where "1" means the last disconnection in T_K.

Case A2c: Again, no re-authentication is needed (Fig. 8(a)). Thus, $E[C_{t_{K'u}}|\text{A2, A2c}] = 0$.

Case A2d: This is similar to Case A2b2, so

$$E[C_{t_{K'u}}|\text{A2, A2d}] = \frac{\lambda_d}{\lambda_u}. \quad (6)$$

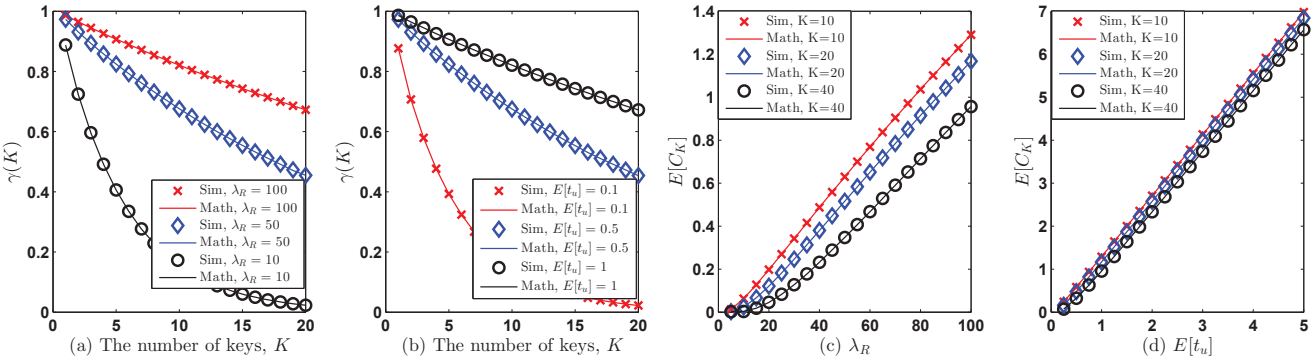
Applying the above cases to Eq. (1), we have:

$$\begin{aligned} &E[C_K] \\ &= \left[\left[1 - \left(\frac{\lambda_R}{\lambda_d + \lambda_R}\right)^K\right] \int_0^\infty \int_s^\infty f_{t'_d}(t) f_{T'_K}(s) dt ds \right. \\ &\quad \left. + \frac{\lambda_d}{\lambda_u} \int_0^\infty \int_s^\infty f_{t'_d}(t) f_{t'_R}(s) dt ds \right] \left(\frac{\lambda_R}{\lambda_u + \lambda_R}\right)^K. \quad (7) \end{aligned}$$

Note that in the original KMM, a UE obtains one key from BM-SC. We can use Eq. (7) to derive its re-authentication count by setting $K = 1$.

B. Expected Free Enjoying Time $E[Free_K]$

We have $E[\text{Free}_K] = E[\text{RemainKey}] \times E\left[\frac{\text{Free\_Using\_Time}}{\text{Key}}\right]$ where $E[\text{RemainKey}] = E[K - 1 - (\text{Rekey within } t_u)] = K - 1 - \frac{\lambda_R}{\lambda_u}$. If $K - 1 - \frac{\lambda_R}{\lambda_u} < 0$, it means that the UE consumes



(a) The number of keys, K (b) The number of keys, K (c) λ_R (d) $E[t_u]$

Fig. 9: The different effects of $\gamma(K)$ and $E[C_K]$ with different parameters

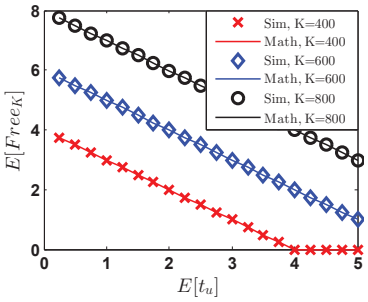


Fig. 10: The effects of $E[t_u]$ on $E[Free_K]$ with different K.

the pre-issue keys completely. $E\left[\frac{\text{Free\_Using\_Time}}{\text{Key}}\right]$ is the excess life time for the next rekey ($\frac{1}{\lambda_R}$). So,

$$E[\text{Free}_K] = (K - 1 - \frac{\lambda_R}{\lambda_u}) \times \frac{1}{\lambda_R}. \quad (8)$$

V. Simulation Validation

In this section, we validates our analytical model by ns2 simulations. The differences between analytical and simulation results fall within 1%. Unless otherwise specified, the following parameter are used: $\lambda_R = 100$/hour, $E[t_u] = 1$ hour, $\lambda_d = 10$/hour, and $E[t'_d] = 6$ sec.

Given different K, Fig. 9(a) and Fig. 9(b) show analytic and simulated $E[C_K]$ and $\gamma(K)$ by varying rekeying rate λ_R and resident time t_u. The simulation results match well with our analytical results. These results all show the effect of increasing K. Given a fixed K, Fig. 9(c) shows the relationship between λ_R and $E[C_K]$. A higher rate λ_R will lead to a larger cost $E[C_K]$ because key updates are more frequent. Given a fixed K, Fig. 9 (d) illustrates the relationship between resident time $E[t_u]$ and $E[C_K]$. Fig. 10 shows that the effect of K and $E[t_u]$ on free enjoying time $E[Free_K]$. All these results validate the correctness of our analyses.

VI. Derivation of the Optimal K

In this section, we discuss the selection of K. In particular, selecting a suitable K to balance the tradeoff is important. Thus, we formulate the objective function as:

$$\begin{aligned} \arg\min_{K} \quad & F = w_1 E[C_K] + w_2 E[Free_K], \\ \text{subject to} \quad & 0 < E[Free_K] \leq \Theta, \end{aligned} \quad (9)$$

where Θ is the upper bound of $E[Free_K]$, which can be determined by content providers according to their business policies. The coefficients of $w1$ and $w2$ denote the weighting factors. Increasing $w1$ (or $w2$) emphasizes more on $E[C_K]$ ($E[Free_K]$). 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 the closed form of $E[C_K]$ and $E[Free_K]$ has been derived in Eq. (7) and Eq. (8), respectively, the optimal value of K can be founded by solving the differential equation $F' = 0$ and $F'' > 0$.

VII. Conclusions

In this paper, we propose KeySet to reduce re-authentication cost by distributing a number of security keys K to a UE conducting authentication procedure. The K keys prevent UE from missing rekeying operation while in disconnection status at cost of free enjoying time. Instead of tuning K randomly, our performance study provides theoretical guidelines and a systematic way for network operators to configure a suitable K. An optimal equation is presented to get the optimal K.

Acknowledgment

The work was done when Yi Ren was with National Chiao Tung Univerisity.

References

[1] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, "Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463–8476, 2016.

[2] Ericsson, "Ericsson mobility report on the pulse of the networked society," Ericsson, Tech. Rep., Jun. 2014.

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

[4] 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'l Conf. Computer Theory and Applications (ICCTA '12)*, 2012, pp. 60–65.

[5] L. Chen and J. Leneutre, "On multipath routing in multihop wireless networks: security, performance, and their tradeoff," *EURASIP J Wirel. Comm.*, p. 6, 2009.

[6] M. Haleem, C. N. Mathur, R. Chandramouli, K. Subbalakshmi *et al.*, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Depend. Secu. Comp.*, vol. 4, no. 4, pp. 313–324, 2007.

[7] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM Mobihoc*, 2010, pp. 21–30.

[8] 3GPP TS 33.246 V14.0.0, *3G security; security of Multimedia Broadcast/Multicast Service (MBMS) (Release 14)*, Std., Dec. 2016.

[9] 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, 2014.