INFORMATION
Volume 18, Number 3, pp.1095-1100

ISSN 1343-4500
©2015 International Information Institute

Optimization of Authentication Cost based on Key Caching for Inter-MME Handover Support

Myungseok Song*, Jun-Dong Cho** and Jongpil Jeong***,

Sungkyunkwan University
2066 Seobu-ro Jangan-gu, Suwon, Kyunggi-do, 440-726, Korea
* *E-mail: bestsong21@hotmail.com*
** *E-mail: jdcho@skku.edu*
*** *E-mail: jpjeong@skku.edu*

Abstract

In the long term evolution (LTE) network environment, a new authentication key must be created during the handover. The authentication process is performed by handover, authentication cost and delay time are caused. In this paper, we propose an efficient key caching handover technique of simplifying the authentication process by reusing the stored authentication key if old mobility management entity (oMME) stores the authentication key for a certain period of time and returns it to oMME within life time of the authentication key when user equipment (UE) is handed over from oMME to New mobility management entity (nMME).

Key Words: Mobile Network, LTE; Handover, Key caching, Authentication Cost

1. Introduction

In the street, consumers can enjoy the download speed of the wired Internet being used in common households. However, some LTE users have recently experienced the problem that the signal is disconnected suddenly when calling. If handover [1,2] does not work properly, call quality problem arises. In order to solve call delay and disconnection phenomenon during the handover pointed out as the biggest problem of the mobile network, many studies for fast and efficient handover have been carried out. A new authentication key must be created when UE is handed over from oMME to nMME in the LTE network environment [3,4]. In this case, oMME will delete the authentication key record of UE. If UE removes and returns to oMME again, authentication cost and delay time will occur because the authentication process is performed by the handover [5,6]. We propose an efficient key caching handover technique of simplifying the authentication process by reusing the stored authentication key if oMME stores the authentication key for a certain period of time and returns it to old MME within Life Time of the authentication key when UE is handed over from oMME to n MME.

2. Authentication cost based on key

In this paper, we propose a handover technique based on key caching for more efficient and faster handover on the LTE network. Fig. 1. depicts MME handover process based on key caching [7]. UE measures signal strength and then if signal strength is weakened, it sends Measurement message to source eNodeB (S-eNB) (1). S-eNB contains information of target eNodeB (T-eNB) in the handover required message and requests handover to MME (2). oMME sends MM Context to nMME through Forward Relocation Request message. MM Context includes Security Context (K_{ASME} , AV, Used NAS security algorithms, NH, NCC) (3). nMME uses it as NAS Security Context for the UE and sends NCC, NH to T-eNB through handover Request message so that T-eNB can obtain KeNB* (4). When connected to its cell through handover Request ACK message,

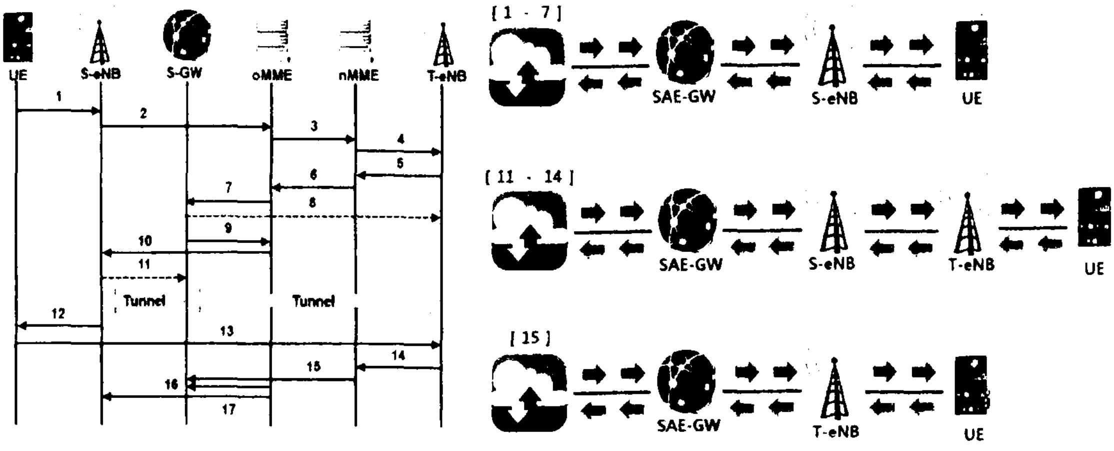

Fig. 1. INTRA-handover based on Key Caching.

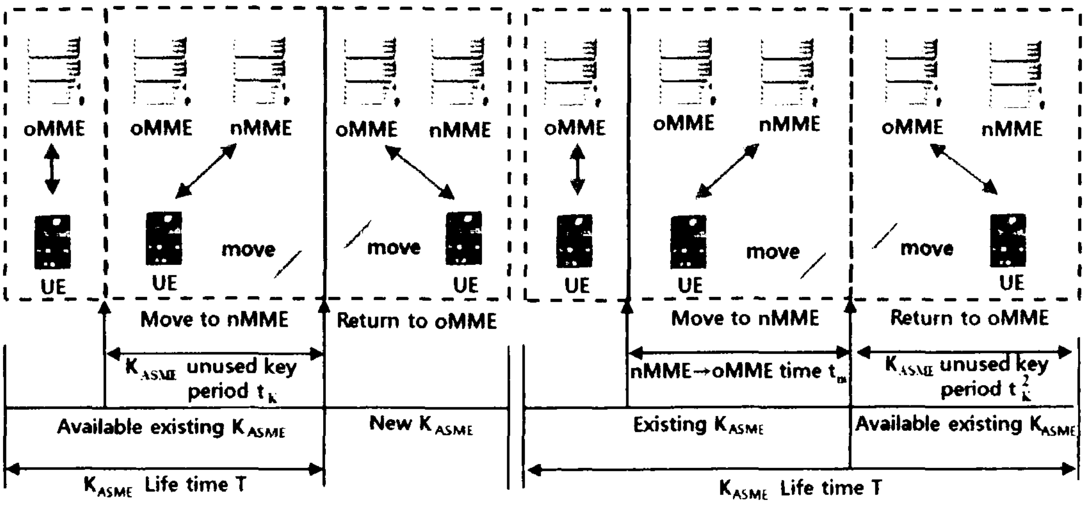

Fig. 2. The case UE does not return before K_{ASME} 's life T Expiration (left) and the case UE return before K_{ASME} 's life T Expiration (right)

T-eNB contains necessary information and sends it to MME (5). nMME sends information of T-eNB to oMME (6). oMME sends information for generating Tunnel to SAE-GW (7). SAE-GW connects Indirect Tunnel to T-eNB (8). SAE-GW sends Tunnel generation information to oMME (9). nMME requests to modify the packet path to SAE-GW and SAE-GW changes the packet path to T-eNB (15). oMME sends UE Context Release Command message to S-eNB to request release of resources assigned to the UE (16). nMME requests to release Indirect Tunnel to SAE-GW (17). If handover is over, Globally Unique Temporary Identifier (GUTI) is assigned by nMME to the UE through tracking area update (TAU) procedure. If the UE returns to oMME again within time of K_{ASME} life T and is handed over, the same operation is repeated and oMME uses NAS security context passed to nMME and therefore, K_{ASME} can be used as it is without re-authentication even if MME is changed during the handover [8].

3. Perforrmance Analysis

We analyze the impact on performance of key caching depending on life time of K_{ASME} value. Fig. 2. show the relationship between movement of the UE and K_{ASME} life time [8]. As shown in Fig. 2. (left), if UE does not return to oMME until life time of K_{ASME} is expired, the period t_K is defined as "K_{ASME} unused key period". UE's separation from existing MME is assumed to occur randomly for K_{ASME} life time. For fixed K_{ASME} life time T value, t_K shows uniform distribution in the section of $0 \le t_K \le T$ by remaining life theory. At this time, α, $E[t_K \mid t_M \ge t_K]$, $E[t^*_K \mid t_M \le t_K]$ value is derived as follows.

$$\alpha = \Pr[t_M \le t_K] = \int_{t_K=0}^{T} \left(\frac{1}{T}\right)\left(\lambda e^{-\lambda t} dt_M\right) dt_K = \frac{e^{-\lambda T} + \lambda T - 1}{\lambda T}, \tag{3.1}$$

Since UE's separation from existing MME was assumed to occur randomly for K_{ASME} life time, t_K can be said to be exponential distribution with mean E[T]= $1/\mu$ based on remaining life theory. Let's suppose that t_M shows random distribution with density function $f(t_M)$ and Laplace Transform Formula f*(s). At this time, α, $E[t_K \mid t_M \ge t_K]$, $E[t^*_K \mid t_M \le t_K]$ value is derived as follows.

$$\alpha = \int_{t_K=0}^{\infty} \mu^{-\mu t_K} \times \left[\int_{t_M=0}^{t_K} f(t_M) dt_M \right] dt_K = f^*(\mu), \tag{3.2}$$

It can be seen that $E[t_K \mid t_M \geq t_K]$ is not affected by distribution of t_M. Let's suppose that t_M follows gamma distribution according to the assumption that has been used in communication modeling. This is the assumption that has been used in communication modeling. t_M following gamma distribution and Laplace conversion with mean $1/\lambda$ variance V_M are as follows.

$$f^*(s) = \left(\frac{1}{\lambda V_M s + 1}\right)^{\frac{1}{\lambda^2 V_M}} \qquad \alpha = f^*(\mu) = \left(\frac{1}{\lambda \mu V_M s + 1}\right)^{\frac{1}{\lambda^2 V_M}} \tag{3.3}$$

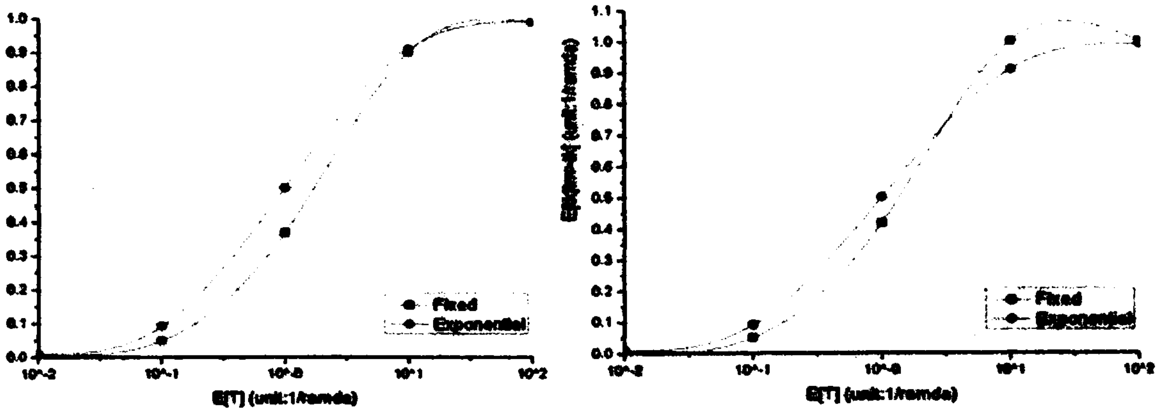

Fig. 3. Comparison of α value (left) and Compare the graph $E[t_K \mid t_M \geq t_K]$ (right)

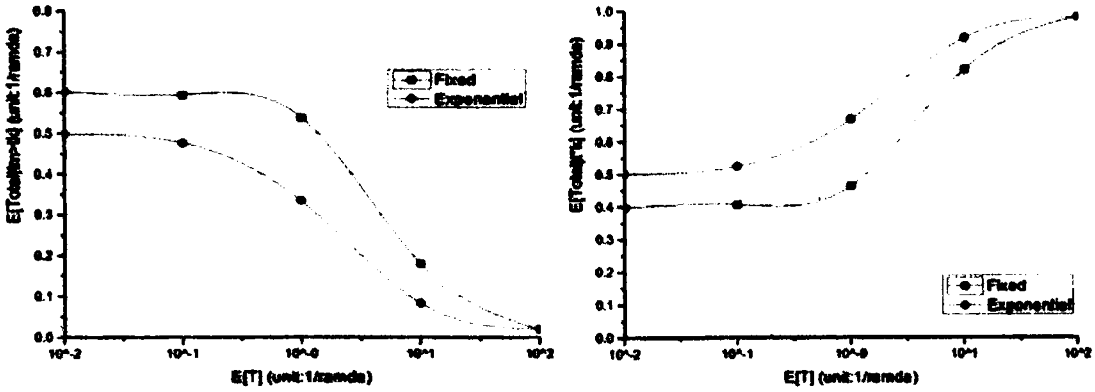

Fig. 4. $E[t_k \mid Total]$ (left) $E[t^*_k \mid Total]$ (right)

Fig. 3. (left) shows the change in α value according to the change in E[T]. According to this graph, α is an increasing function for E[T]. If E[T] gets bigger, it can be seen that UE is highly likely to return to oMME before K_{ASME} life is expired. And it tells us that exponential distribution T shows better α value than fixed T. Fig. 3. (right) expresses $E[t_K \mid t_M \geq t_K]$, unused key period as a function for E[T]. Looking at the graph, it can be seen that unused key period is also increasing as E[T] is increasing Fig. 4. (left) shows the mean of unused time of K_{ASME} for the overall mean considering two cases. Fig. 4. (right) shows the mean of reused time of K_{ASME} for the overall mean considering two cases.

4. Conclusion

In this paper, we proposed key caching mechanism for efficient handover on the LTE network. The proposed mechanism is a technique for simplifying the authentication process that UE reuses K_{ASME} stored in oMME if oMME stores K_{ASME} of UE when UE is handed over from oMME to nMME and UE returns to oMME before life time of K_{ASME} is expired. Also, by analyzing efficiency depending on life time of K_{ASME}, we proposed efficient key caching mechanism while not wasting the storage memory of K_{ASME}. AS a result, it can be seen that performance is excellent when T value shows exponential distribution than T value is fixed.

References

[1] DongHwi, K. and Jongpil, J., Analytical Approach of Cross-Layer-Based Handoff Scheme in Heterogeneous Mobile Networks., *The Journal of The Institute of Webcasting, Internet and Telecommunication,* 13:6 (2013), 1-16.

[2] Illkyun, I. and Jongpil, J., Authentication eXtention Scheme of Fast Handover for Secure NEMO-based PMIPv6 Networks., *The Journal of The Institute of Webcasting, Internet and Telecommunication,* 13:5 (2013), 107-119.

[3] 3GPP TS 36.331., Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification.

[4] H. Yi, S. Kim, and J. Choi, Analysis of TCP Performance in LTE Wireless Network. *Journal of Korean Institute of Information Technology.* 11:5 (2013), 97-104.

[5] 3GPP TS 36.423 V8.0.0 (2007-12)., Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP).

[6] 3GPP TS 36.331 V9.3.0 (2010-06)., E-UTRA; RRC; Protocol specification.

[7] Hsu, Shih-Feng. etc., A Key Caching Mechanism for Reducing WiMAX Authentication Cost in Handoff. *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.* 58:8 (2009), 4507-4513.

[8] 3GPP TS 33.401 v8.1.1 (2008-10)., 3GPP System Architecture Evolution (SAE); Security Architecture.

**Corresponding author: Jun-Dong Cho, Ph.D.
Department of Human ICT Convergence,
Sungkyunkwan University,
Suwon, Kyunggi-do, Republic of Korea,
E-mail: jdcho@skku.edu