http://dx.doi.org/10.7236/JIIBC.2013.13.5.209
JIIBC 2013-5-26

MME 도메인간 핸드오버 지원을 위한 키캐싱 기반 인증비용의 감소기법

Reduction of Authentication Cost Based on Key Caching for Inter-MME Handover Support

황학선*, 정종필**

Hakseon Hwang, Jongpil Jeong

요 약 핸드오버는 통신 중인 무선 단말이 데이터의 손실을 최소화 하면서 현재 접속하고 있는 기지국/셀에서 다른 기지국/셀로 이동을 하여도 연속적으로 통신이 가능하게 하는 기술이다. 즉, 이동통신 가입자가 특정 무선통신 구역에서 다른 무선통신 구역으로 이동할 때, 통화 채널을 자동으로 전환시켜 통화를 끊어지지 않게 해주는 기능을 말한다. 현재 모바일 네트워크의 가장 큰 문제점으로 지적되고 있는 핸드오버 시 통화 지연 현상 및 끊김 현상을 해결하기 위해 빠르고 효율적인 핸드오버를 위한 많은 연구가 진행되고 있으며, 이러한 통화지연 및 끊김 현상은 모든 모바일 네트워크에서 필수적으로 해결해야 할 부분이다. 최근 모바일 네트워크의 기술 발달로 LTE(Long Term Evolution) 네트워크가 상용화되어 모바일에서도 고속의 데이터처리가 가능한 시대를 열었다. 하지만 LTE 네트워크 환경에서는 핸드오버 시 새로운 인증키가 생성되어야 한다. 이런 경우 핸드오버에 의해 인증 과정이 수행되어 인증 비용 및 지연시간이 발생하는 문제점이 있다.본 논문에서는 UE가 oMME에서 nMME로 핸드오버 시 oMME는 인증키를 일정 시간 동안 저장하여 인증키의 Life Time내에 기존의 MME로 다시 복귀한다면 저장된 인증키를 재사용을 하여 인증 절차를 간소화하는 효율적인 키캐싱 핸드오버 기법을 제안한다.

Abstract Handover is the technology to minimize data lose of mobile devices and make continuous communication possible even if the device could be moved from one digital cell site to another one. That is, it is a function that enables the mobile user to avoid the disconnection of phone conversations when moving from a specific mobile communication area to another. Today, there are a lot of ongoing researches for fast and efficient hand-over, in order to address phone call's delay and disconnection which are believed to be the mobile network's biggest problems, and these should essentially be resolved in all mobile networks. Thanks to recent technology development in mobile network, the LTE network has been commercialized today and it has finally opened a new era that makes it possible for mobile phones to process data at high speed. In LTE network environment, however, a new authentication key must be generated for the hand-over. In this case, there can be a problem that the authentication process conducted by the hand-over incurs its authentication cost and delay time. This essay suggests an efficient key caching hand-over method which simplifies the authentication process: when UE makes hand-over from oMME to nMME, the oMME keeps the authentication key for a period of time, and if it returns to the previous MME within the key's lifetime, the saved key can be re-used.

Key Words : Mobile Network, LTE, Handover, Key caching,

*정회원, 성균관대학교 컴퓨터공학과
**정회원, 성균관대학교 정보통신대학 (교신저자)
접수일자: 2013월 9월 26일, 수정완료: 2013년 10월 8일
게재확정일자: 2013년 10월 11일

Received: 26 September, 2013 / Revised: 8 October, 2013
Accepted: 11 October, 2013
**Corresponding Author: jpjeong@skku.edu
Colleage of Information and Communication Engineering, Sungkyunkwan University, Korea

Ⅰ. 서 론

우리나라 휴대전화는 과거 아날로그 방식(1세대)에서 CDMA(2세대), WCDMA(3세대), 그리고 최근의 LTE(4세대)로 발전해 왔다. 통신 방식의 발전은 데이터 다운로드/업로드 속도에도 변화를 가져왔는데, 이론상 현 LTE는 과거 WCDMA 대비 최대 5배 빠른 것이 장점이다. 길거리에서도 일반 가정에서 사용 중인 유선인터넷의 다운로드 속도를 만끽할 수 있게 되었다. 그러나 최근 일부 LTE 사용자들은 통화 시 갑자기 신호가 끊어지는 문제가 발생한다는 불만을 토로하고 있다. LTE 데이터를 이용하다 전화통화를 할 때 통화 품질 저하되는 현상이 발생하고 있다.핸드오버는 통신 신호를 받고 있는 모바일 단말기가 다른 기지국 신호를 잡거나 혹은 통신 방식이 변경될 때 지속적으로 통화가 유지되도록 하는 기술이다. '핸드오버'가 정상적으로 작동되지 않으면 통화 품질에 문제가 발생한다.

본모바일 네트워크의 가장 큰 문제점으로 지적되고 있는 핸드오버 시 통화 지연 현상 및 끊김 현상을 해결하기 위해 빠르고 효율적인 핸드오버를 위한 많은 연구가 진행되고 있다. 이러한 통화지연 및 끊김 현상은 모든 모바일 네트워크에서 필수적으로 해결해야 할 부분이다. 최근 모바일 네트워크의 기술 발달로 LTE(Long Term Evolution) 네트워크가 상용화되어 모바일에서도 고속의 데이터처리가 가능한 시대를 열었다. 하지만 LTE 네트워크 또한 핸드오버 시 통화 지연 현상 및 끊김 현상은 여전히 해결해야 하는 과제이다.

LTE 네트워크 환경에서는 UE(User Equipment)가 oMME(Old Mobility Management Entity)에서 nMME(New Mobility Management Entity)로 핸드오버 시 새로운 인증키가 생성되어야 한다[1] . 이런 경우 oMME는 UE의 인증키 레코드를 삭제 할 것이다. UE가 재이동하여 다시 oMME로 복귀한다면, 핸드오버에 의해 인증 과정이 수행되어 인증 비용 및 지연시간이 발생 할 것이다.[2],[3] 핸드오버는 통신 신호를 받고 있는 모바일 단말기가 다른 기지국 신호를 잡거나 혹은 통신 방식이 변경될 때 지속적으로 통화가 유지되도록 하는 기술이다. '핸드오버'가 정상적으로 작동되지 않으면 통화 품질에 문제가 발생한다.

본 논문에서는 UE가 oMME에서 nMME로 핸드오버 시 oMME는 인증키를 일정 시간 동안 저장하여 인증키의 Life Time내에 기존의 MME로 다시 복귀한다면 저장된 인증키를 재사용을 하여 인증 절차를 간소화하는 효율적인 키캐싱 핸드오버 기법을 제안한다. 제안하는 기법은 인증키의 Life Time에 따른 효율성을 분석하여 인증키의 저장 메모리의 낭비를 최소화 하였다.

본 논문의 구성은 다음과 같다. Ⅱ 장에서는 LTE 네트워크에서의 핸드오버 과정과 인증과정에 대해 알아보고 Ⅲ 장에서는 본 논문에서 제안하는 키캐싱에 기반한 MME간 핸드오버 인증에 대해 설명한다. Ⅳ 장에서는 시스템 모델링을 통해 인증키의 Life Time에 따른 효율성을 분석한다. 마지막 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

1. LTE 네트워크에서의 핸드오버

만약 UE가 현재 통신하고 있는 기지국/셀에서 새로운 기지국/셀로 이동하였다면 끊김 없는 서비스를 제공하기 위해서는 핸드오버가 발생되어야 한다. 그림 1은 LTE 네트워크에서의 핸드오버 과정을 나타낸 것이다.[4],[9]

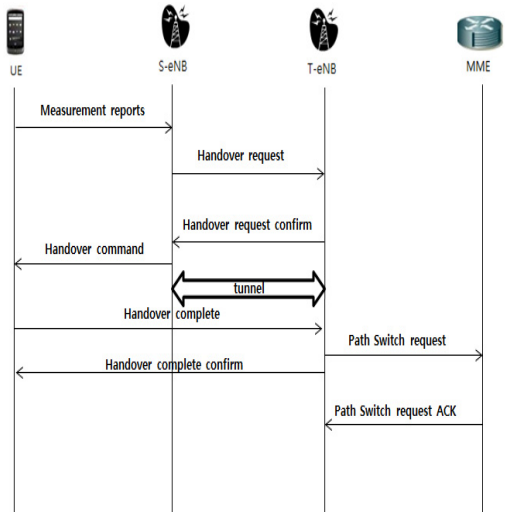


그림 1. LTE 네트워크의 핸드오버 과정
Fig. 1. Handover process of LTE networks

(1) Measurement 단계

UE는 서비스하는 기지국/셀과 주변 기지국/셀들의 수신 신호의 세기를 측정하고 있다가 event가 발생하 면 Measurement Report 메시지를 통해 측정값을

S-eNB(Evolved Node B)에게 전달한다.

(2) Handover Decision 단계

Event가 보고되면 S-eNB는 UE에게 수신한 Measurement Report 메시지의 Eevent 정보와 자신이 관리하고 있는 주변 기지국/셀 정보를 기반으로 어떤 종류의 핸드오버를 할지 결정한다. 핸드오버 종류는 표 1과 같다.

표 1. LTE 네트워크의 핸드오버 종류
Table 1. Kind of LTE networks Handover

Handover 영역에 따른 분류	Handover 유형	특징
Intra-LTE Handover	Intra-MME/ S-GW (Serving Gateway) Handover	핸드오버 전/후에 MME와 S-GW가 변경되지 않고 eNB만 변경되는 경우
Inter-LTE Handover	Inter-MME Handover	핸드오버 전/후에 eNB 와 MME가 변경되는 핸드오버
	Inter-S-GW Handover	핸드오버 전/후에 eNB 와 S-GW가 변경되는 핸드오버
	Inter-MME/ S-GW Handover	핸드오버 전/후에 eNB 와 MME와 S-GW가 모두 변경되는 핸드오버
Inter-RAT Handover	UTRAN to E-UTRAN E-UTRAN to UTRAN	LTE에서 다른 기술 간의 핸드오버 (Ex 3G <-> LTE)

(3) Handover Prepartion 단계

S-eNB는 T-eNB에게 Handover Request 메시지 통해 UE Context를 전송하고 서비스 품질을 확인한다. T-eNB는 UE가 사용 할 DRB 자원 및 C-RNTI (Cell-Radio network Temporary Identity)를 할당 하여 S-eNB에게 Handover Request Confirm 메시지를 보낸다.

(4) Handover Execution 단계

UE가 핸드오버를 실행하는 단계로 S-eNB는 UE에게 Handover Command 메시지를 통해 T-eNB에 접속하는데 필요한 정보를 전송하고 핸드오버를 지시한다. 메시지를 수신한 UE는 S-eNB와의 접속을 끊고 T-eNB에게 접속 한다. 이때 S-eNB와 T-eNB사이에 Tunnel을 생성하여 UL/DL(Uplink/Downlink)패킷이 손실되는 것을 막는다.

(5) Handover Completion

T-eNB는 UE가 정상적으로 접속을 성공하면 S-eNB와 T-eNB의 Tunnel을 통해 전송 받았던 패킷 경로를 T-eNB로 변경하고 Tunnel을 해제한다.

2. LTE 네트워크에서의 인증

UE가 LTE 네트워크에 접속 요청을 하면 EPS(Evolved Packet System) AKA(Authentication and Key Agreement) 절차를 통해 UE와 MME, HSS(Home Subscriber Server)간의 LTE 네트워크 상호 인증이 발생된다. 그림 2는 LTE 네트워크의 인증 과정을 나타낸 것이다.

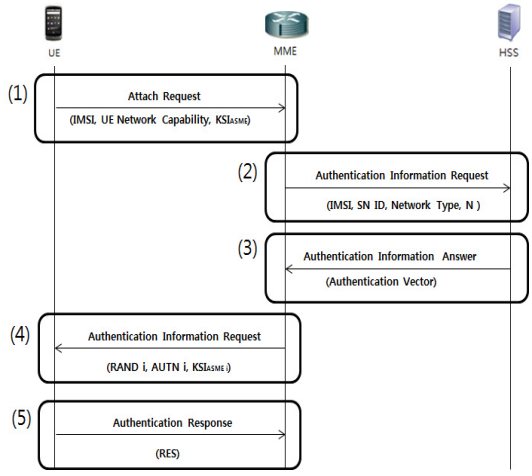


그림 2. LTE 네트워크의 인증 과정
Fig. 2. Certification process of LTE networks

(1) UE는 MME에게 접속 요청을 하는 단계로 Attach Request 메시지를 전송한다. Attach Request 메시지에는 IMSI(International Mobile Subscriber Identity), UE Network Capability, KSIASME (Key Set Identifier Access Security Management Entity) 정보들이 포함되어 있다.

(2) UE의 접속 요청을 받은 MME는 HSS에게 Authentication Information Request 메시지를 전송하고 해당 가입자의 인증데이터를 요청한다. Authentication Information Request 메시지에는 IMSI, SN ID(Serving Network ID), Network

Type, N(Number of Authentication Vector)의 정보가 포함되어 있으며 HSS는 수신한 정보를 가지고 KASME 생성하고 인증 벡터(RANDn (Random Number), AUTNn(Authentication Token), XRESn,(Expected Response), KASMEn)를 구성한다.

(3) HSS는 Authentication Information Anwer 메시지를 통해 MME에게 인증 백터 (RANDn, AUTNn, XRESn, KASMEn)를 전달한다.

(4) MME는 인증 벡터 중 KASMEi와 XRESi 값은 저장하고 Authentication Request 메시지 통해 (RANDi, AUTNi, KSIASME)값을 UE에게 전달한다. UE는 AKA 알고리즘을 사용하여 생성한 AUTH값과 MME 에게 전송받은 AUTH 값을 비교하여 같으면 망 인증을 한다.

(5) 망 인증을 마친 후 UE는 MME가 사용자 인증을 할 수 있도록 Authentication Response를 통해 RES(Response)를 전달하고 MME는 HSS로부터 받은 XRES 와 같은지 비교하여 사용자 인증을 한다.[5]

Ⅲ. 키캐싱에 기반한 MME간 핸드오버 인증비용의 감소 기법

본 논문에서는 LTE 네트워크에서의 핸드오버를 더 효율적이고 빠르게 진행하기 위해서 키캐싱에 기반한 핸드오버 기법을 제안한다.

oMME와 nMME가 같은 PLMN에 있고 동일한 보안 알고리즘을 사용한다고 가정한다. UE가 oMME에서 nMME로 이동 할때 oMME는 할당받았던 KASME값을 일정시간 동안 보유한다. 만약 UE가 KASME의 수명이 만료되기 전에 oMME로 복귀한다면 인증을 다시 거치지 않고 KASME를 재사용하여 빠른 핸드오버를 수행할 수 있다. 이때 KASME의 수명이 너무 길면 인증비용이 많이 들고, KASME값을 저장하기 위한 메모리도 낭비된다. 따라서 적절한 KASME의 수명을 선택하는 것이 바람직하다. 다음 그림 3은 LTE 네트워크에서 키캐싱을 이용한 핸드오버 과정을 나타낸 것이다.[6]

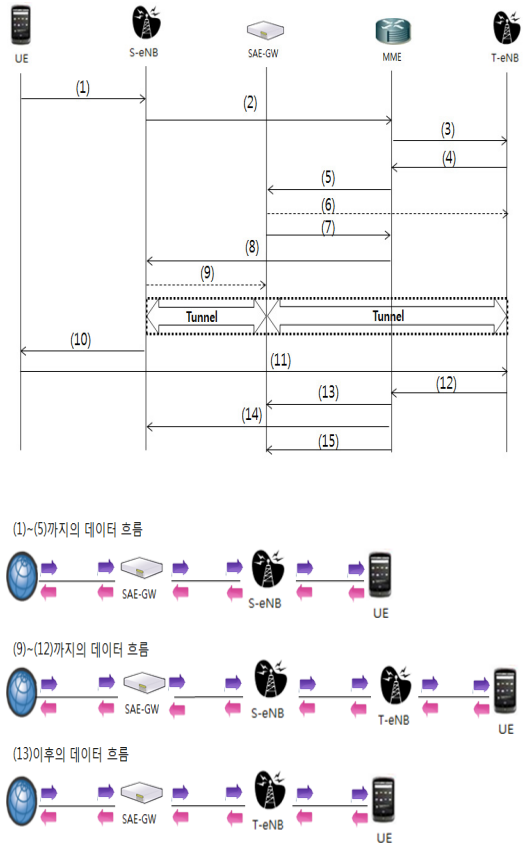


그림 3. 키캐싱에 기반한 INTRA-핸드오버
Fig. 3. INTRA-Handover based on Key Caching

(1) UE는 신호세기를 측정하고 있다가 신호 세기가 약해지면 Measurement 메시지를 S-eNB 에게 전송한다.

(2) S-eNB는 Handover Required 메시지에 T-eNB의 정보를 담아 MME에게 핸드오버를 요청을 한다.

(3) MME는 Handover Required 메시지를 통해 UE Context 정보를 포함하여 T-eNB에게 핸드오버를 요청한다.

(4) T-eNB는 Handover Request ACK 메시지 를 통해 자신의 셀로 접속할 때 필요한 정보를 포함하여 MME에게 전송한다.

(5) MME는 Tunnel을 생성하기 위한 정보를 SAE-GW에게 전달한다.

(6) SAE-GW는 T-eNB에게 Indirect 터널을 연 결한다.

(7) SAE-GW는 Tunnel 생성 정보를 MME에게 전송

한다.

(8) MME는 S-eNB에게 SAE-GW로 Indirect 터널을 생성하기 위한 정보와 UE가 T-eNB로 접속하기 위한 정보를 전송한다.

(9) S-eNB는 수신한 정보를 바탕으로 SAE-GW로 Indirect 터널을 연결한다. 이 과정을 거쳐 S-eNB - SAE-GW - T-eNB 구간의 Indirect 터널이 생성된다.

(10) 핸드오버를 위한 준비가 완료 되었으므로 S-eNB는 T-eNB로 핸드오버하기 위해 필요한 정 보를 Handover Command 메시지를 통해 UE에게 전송하고 핸드오버를 지시한다.

(11) UE는 S-eNB와 접속을 끊고 T-eNB로 접속한다.

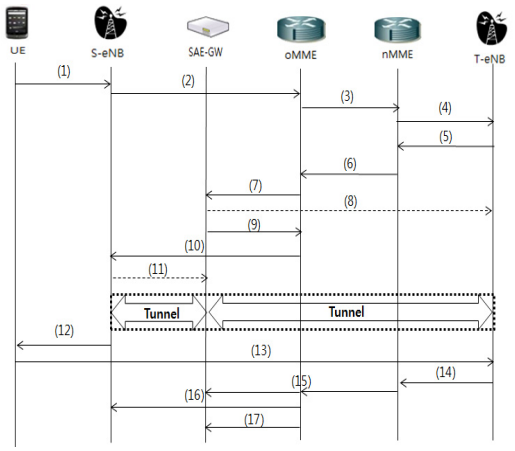
(12) T-eNB는 MME에게 Handover Notify 메시지를 전송하여 UE가 핸드오버를 성공했음을 알린다.

(13) MME는 SAE-GW에게 패킷 경로를 수정 요청하고 SAE-GW는 패킷 경로를 T-eNB로 변경한다.

(14) MME는 UE Context Release Command 메시지를 S-eNB에게 전송하여 UE에 할당된 자원의 해제를 요청한다.

(15) 마지막으로 MME는 SAE-GW에게 Indirect 터널을 해제할 것을 요청한다.

그림 4는 키캐싱에 기반한 MME 핸드오버과정을 나타 낸 것이다.[7]



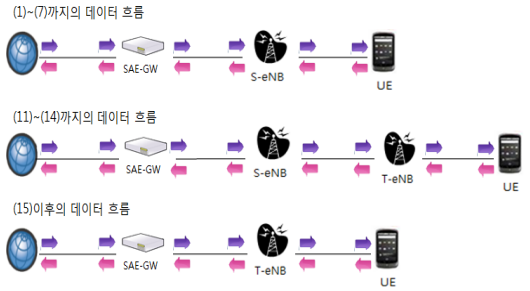


그림 4. 키캐싱에 기반한 INTRA-핸드오버
Fig. 4. INTRA-Handover based on Key Caching

(1) UE는 신호세기를 측정하고 있다가 신호 세기가가 약해지면 Measurement 메시지를 S-eNB에게 전송한다.

(2) S-eNB는 Handover Required 메시지에 T-eNB의 정보를 담아 MME에게 핸드오버를 요청을 한다.

(3) oMME는 nMME에게 Forward Relocation Request 메시지를 통해 MM Context 전달한다. MM Context에는 Security Context (KASME, AV, Used NAS security algorithms, NH, NCC)가 포함되어 있다.

(4) nMME는 이를 UE에 대한 NAS Security Context로 사용하고, T-eNB에게 Handover Request 메시지를 통해 NCC, NH를 전송하여 T-eNB가 KeNB*를 구할 수 있게 한다,

(5) T-eNB는 Handover Request ACK 메시지를 통해 자신의 셀로 접속할 때 필요한 정보를 포함하여 nMME에게 전송한다.

(6) nMME는 T-eNB의 정보를 oMME에게 전달한다.

(7) oMME는 Tunnel을 생성하기 위한 정보를 SAE-GW에게 전달한다.

(8) SAE-GW는 T-eNB에게 Indirect 터널을 연결한다.

(9) SAE-GW는 Tunnel 생성 정보를 oMME에게 전송 한다.

(10) oMME는 SAE-GW로 Indirect 터널을 생성하기 위한 정보와 UE가 T-eNB로 접속하기 위한 정보를 S-eNB에게 전송한다.

(11) S-eNB는 수신한 정보를 바탕으로 SAE-GW로 Indirect 터널을 연결한다. 이 과정을 거쳐 S-eNB - SAE-GW - T-eNB 구간의 Indirect 터널이 생성된다.

(12) 핸드오버를 위한 준비가 완료 되었으므로 S-eNB는 Handover Command 메시지를 통해 T-eNB로 핸드오버하기 위해 필요한 정보를 UE에게 전송하고 핸드오버를 지시한다.

(13) UE는 S-eNB와 접속을 끊고 T-eNB로 접속 한다.

(14) T-eNB는 nMME에게 Handover Notify 메시지를 전송하여 UE가 핸드오버를 성공했음을 알린다.

(15) nMME는 SAE-GW에게 패킷 경로를 수정 요청하고 SAE-GW는 패킷 경로를 T-eNB로 변경한다.

(16) oMME는 UE Context Release Command 메시지를 S-eNB에게 전송하여 UE에 할당된 자원의 해제를 요청한다.

(17) nMME는 SAE-GW에게 Indirect 터널을 해제할 것을 요청한다.

핸드오버가 끝나면 UE는 TAU 절차를 통해 nMME로부터 GUTI를 할당받는다. 만약 KASME 수명 T의 시간 내에 다시 oMME로 복귀하여 핸드오버를 한다면, 같은 동작이 반복되며 oMME는 nMME에게 전달받은 NAS security context를 사용하므로 핸드오버 시 MME가 변경 되어도 재인증 없이 KASME가 그대로 사용할 수 있다.[8]

Ⅳ. 성능 분석

1. 시스템 모델링

KASME값의 수명에 따라서 키캐싱의 성능에 미치는 영향을 분석한다. 그림 3, 그림 4는 UE의 이동과 KASME 수명간의 관계를 보여주고 있다.[8]

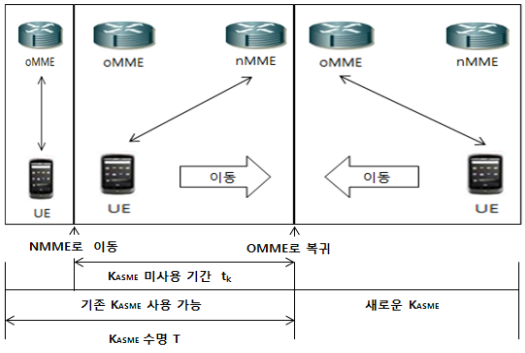


그림 4. UE가 KASME의 수명 T가 만료 전에 복귀하지 않는 경우

Fig. 4. The case UE does not return before KASME's life T Expiration

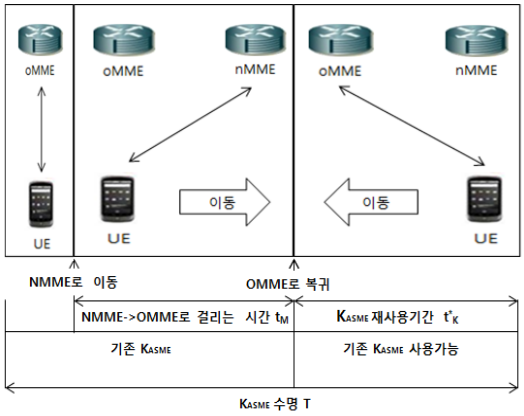


그림 5. UE가 KASME의 수명 T가 만료 전에 복귀하는 경우

Fig. 5. The case UE return before KASME's life T Expiration

그림 4와 같이 KASME의 수명이 만료될 때까지 UE가 oMME로 복귀하지 않는 경우, 이때의 기간 tk를 "KASME 미사용 키 기간" 이라고 정의한다. 또한 그림 5와 같이 KASME의 수명이 만료되기 전에 UE가 oMME로 복귀하는 경우, tM을 "UE가 oMME를 떠나 nMME로 이동했다가 다시 복귀하는데 걸리는 시간", t*K를 "KASME 재사용키 기간" 이라고 정의한다. 또한 KASME의 수명 T는 비율 μ를 가지는 지수 분포이거나, 고정 값을 가지며, UE가 nMME에 머문 시간 tM은, 평균 1/λ 및 분산 VM인 밀도 함수 f(tM)으로 표현된다고 가정한다.

본 논문에서는 다음과 같이 세 가지 값을 계산하여 성능을 평가하였다.

1) α : KASME 수명이 만료되기 전에 UE가 oMME로 복귀할 확률.

2) E[tk|tM≥tk] : KASME 수명이 만료될 때까지 oMME로 돌아오지 않는 경우, 미사용 키 기간의 평균값.

3) E[t*k|tM≤tk] : KASME수명이 만료되기 전에 이전의 MME로 복귀하는 경우, 재사용키 기간의 평균값. UE가 기존의 MME를 이탈하는 것은, KASME 수명에 대해 무작위로 발생한다고 가정한다. 고정된 KASME 수명 T값 에 대해, tK는 잔여 수명 이론에 의해, 0≤tK≤T 의 구간에서 균등 분포를 보인다. 이때 α, E[tk|tM≥tk], E[t*k|tM≤tk] 값은 다음과 같이 도출된다.

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

$E[t_K | t_M \ge t_K] = \frac{E[t_K \text{and} t_M \ge t_K]}{\Pr[t_M \le t_K]}$이며,

$$E[t_K \text{ and } t_M \ge t_K]$$
$$= \int_{t_M=0}^{T} \lambda e^{-\lambda t_M} \times \left[\left(\int_{t_K=0}^{t_M} t_K \times \left(\frac{1}{T}\right) dt_K\right)\right] dt_M$$
$$+ \int_{t_M=0}^{T} \lambda e^{-\lambda t_M} \times \left[\left(\int_{t_K=0}^{t_M} t_K \times \left(\frac{1}{T}\right) dt_K\right)\right] dt_M$$
$$= \frac{1 - e^{-\lambda t}}{\lambda^2 T} - \frac{e^{-\lambda t}}{\lambda}$$
$$\Pr[t_M \ge t_K] = 1 - \alpha = 1 - \frac{e^{-\lambda t} + \lambda T - 1}{\lambda T}$$

$$E[t_K | t_M \ge t_K]$$
$$= \left(\frac{1 - e^{-\lambda t}}{\lambda^2 T} - \frac{e^{-\lambda t}}{\lambda}\right)\left(\frac{1}{1 - \frac{e^{-\lambda t} + \lambda T - 1}{\lambda T}}\right)$$
$$= \frac{1}{\lambda} - \frac{\lambda e^{-\lambda t}}{1 - e^{-\lambda t}} \quad (2)$$

$$E\left[t_K^* | t_M \le t_K\right] = \frac{E\left[t_K^* \text{ and } t_M \le t_K\right]}{Pr\left[t_M \le t_K\right]}$$

이며

$$E\left[t_K^* \text{ and } t_M \le t_K\right]$$
$$= \int_{t_K=0}^{T} \left(\frac{1}{T}\right)\left[\int_{t_M=0}^{t_K} (t_k - t_M)\lambda e^{-\lambda t_M} dt_M\right] dt_K$$
$$= \frac{T}{2} - \frac{1}{\lambda} + \frac{1 - e^{-\lambda T}}{\lambda^2 T}$$
$$Pr[t_M \le t_K] = \frac{e^{-\lambda t} + \lambda T - 1}{\lambda T}$$

$$E[t_K^* | t_M \le t_K]$$
$$= \left(\frac{T}{2} - \frac{1}{\lambda} + \frac{1 - e^{-\lambda T}}{\lambda^2 T}\right)\left(\frac{1}{\frac{e^{-\lambda t} + \lambda T - 1}{\lambda T}}\right)$$
$$= \frac{\lambda T^2}{2(\lambda T + e^{-\lambda T} - 1)} - \frac{1}{\lambda} \quad (3)$$

UE가 기존의 MME에서 이탈하는 것을, KASME수명에 대해 무작위로 발생한다고 가정했으므로, 잔여 수명 이론으로부터, tk는 평균 E[T]=1/μ 인 지수 분포라 할 수 있다. tM은 밀도함수 f(tM)와 라플라스 변환식 f*(s)을 가지는, 임의의 분포를 보인다고 하자. 이때 a, E[tk|tM≥tk], E[t*k|tM≤tk]값은 다음과 같이 도출된다.

$$a = \int_{t_K=0}^{\infty} \mu^{-\mu t_K} \times \left[\int_{t_M=0}^{t_K} f(t_M) dt_M\right] dt_K$$
$$= f^*(\mu). \quad (4)$$

$$E[t_K | t_M \ge t_K] = \frac{E[t_K \text{and} t_M \ge t_K]}{\Pr[t_M \ge t_K]}$$

이며,

$$E[t_K \text{and} t_M \ge t_K]$$
$$= \int_{t_M=0}^{\infty} f(t_M)\left(\int_{t_K=0}^{t_M} t_K \mu e^{-\mu t_K} dt_K\right) dt_M$$
$$= \frac{1}{\mu} + \left[\frac{df^*(s)}{ds}\right]|_{s=\mu} - \frac{f^*(\mu)}{\mu}$$
$$\Pr[t_M \ge t_K] = 1 - a = 1 - f^*(\mu)$$

$$E\left[t_K^* | t_M \le t_K\right] = \frac{E\left[t_K^* \text{ and } t_M \le t_K\right]}{Pr\left[t_M \le t_K\right]}$$
$$E[t_K | t_M \ge t_K]$$
$$= \left\{\frac{1}{\mu} + \left[\frac{df^*(s)}{ds}\right]|_{s=u} - \frac{f^*(\mu)}{\mu}\right\} \times \left[\frac{1}{1 - f^*(\mu)}\right] \quad (5)$$

이며,

$$E\left[t_K^* \text{and} t_M \le t_K\right]$$
$$= \int_{t_K=0}^{\infty} \mu e^{-\mu t_K} \times \left[\int_{t_M=0}^{t_K} (t_K - t_M) f(t_M) dt_M\right] dt_K = \frac{f^*(\mu)}{\mu}$$
$$Pr\left[t_M \le t_K\right] = f^*(\mu)$$

$$E\left[t_K^* | t_M \le t_K\right] = \frac{f^*(\mu)}{\mu} \times \frac{1}{f^*(\mu)} = \frac{1}{\mu} \quad (6)$$

식(6)을 보면 E[t*k|tM≤tk] 이 tM의 분포에 영향을 받지 않는 것을 알 수 있다.

통신 모델링에서 사용되어온 가정에 따라 tM이 감마 분포를 따른다고 가정하자. 이것은 통신 모델링에서 사용되어온 가정이다. 감마 분포를 따르는 tM은 평균 1/λ, 분산 VM,인 라플라스 변환은 다음을 같다.

$$f^*(s)=\left(\frac{1}{\lambda V_M s+1}\right)^{\frac{1}{\lambda^2 V_M}}$$

이를 이용하여 수식(4)는 다음과 같다.

$$\alpha = f^*(\mu)=\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}} \qquad (7)$$

수식 (5)와 (7)을 이용하여 E[tk|tM≥tk]는 다음과 같다.

$$\begin{aligned} &E[t_K|t_M \geq t_K] \\ &= \left\{\frac{1}{\mu}+\left[\frac{df^*(s)}{ds}\right]|_{s=\mu}-\frac{f^*(\mu)}{\mu}\right\}\times \\ &\quad \left[\frac{1}{1-f^*(\mu)}\right] \\ &= \left[\frac{1}{\mu}-\frac{1}{\lambda}\times\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}+1}-\frac{1}{\mu}\right. \\ &\quad \left.\times\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}}\right] \\ &\quad \times\left[\frac{1}{1-\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}}}\right] \end{aligned} \qquad (8)$$

t_M이 지수 분포를 보일 때, (즉, VM=$\frac{1}{\lambda^2}$ 이라고 한다면) (7), (8) 수식은 다음과 같이 변형된다.

$$\alpha=\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}}=\frac{\lambda}{\lambda+\mu} \qquad (9)$$

$$\begin{aligned} &E[t_K|t_M \geq t_K] \\ &= \left[\frac{1}{\mu}-\frac{1}{\lambda}\times\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}+1}-\frac{1}{\mu}\right. \\ &\quad \left.\times\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}}\right] \\ &\quad \times\left[\frac{1}{1-\left(\frac{1}{\lambda\mu V_M+1}\right)^{\frac{1}{\lambda^2 V_M}}}\right] \\ &= \frac{1}{\lambda+\mu} \end{aligned} \qquad (10)$$

(1),(2),(3),(6),(9),(10) 수식들을 통해 세 가지 분석값의 추세를 알아 볼 수 있다. 표 2, 표3, 표 4는 위 수식을 이용하여 분석한 값을 나타낸 것이며 그림 6, 그림 7, 그림 8은 분석값을 그래프로 나타낸 것이다.

표 2. α값
Table 2. Value of α

E[T]	FIXED T	EXPONENTIAL T
$10^{-2}(\frac{1}{\lambda})$	0.004983	0.00990
$10^{-1}(\frac{1}{\lambda})$	0.048374	0.09090
$10^{0}(\frac{1}{\lambda})$	0.367879	0.5
$10^{1}(\frac{1}{\lambda})$	0.900005	0.90909
$10^{2}(\frac{1}{\lambda})$	0.99	0.99009

표 3. E[tk|tM≥tk]값
Table 3. Value of E[tk|tM≥tk]

E[T]	FIXED T	EXPONENTIAL T
$10^{-2}(\frac{1}{\lambda})$	0.005075	0.00990
$10^{-1}(\frac{1}{\lambda})$	0.049171	0.09090
$10^{0}(\frac{1}{\lambda})$	0.418024	0.5
$10^{1}(\frac{1}{\lambda})$	0.999546	0.90909
$10^{2}(\frac{1}{\lambda})$	1.0	0.99009

표 4. E[tk|tM≤tk]값
Table 4. Value of E[tk|tM≤tk]

E[T]	FIXED T	EXPONENTIAL T
$10^{-2}(\frac{1}{\lambda})$	0.003336	0.01
$10^{-1}(\frac{1}{\lambda})$	0.033609	0.1
$10^{0}(\frac{1}{\lambda})$	0.359141	1.0
$10^{1}(\frac{1}{\lambda})$	4.555528	10
$10^{2}(\frac{1}{\lambda})$	49.505051	49.505051

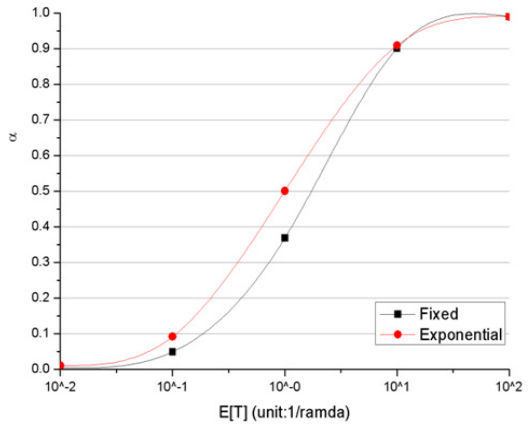


그림 6. α 값 비교
Fig. 6. Comparison of α value

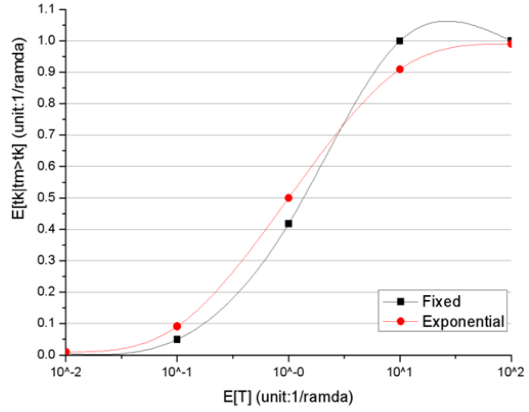


그림 7. E[tk|tM≥tk] 그래프 비교
Fig. 7. Compare the graph E[tk|tM≥tk]

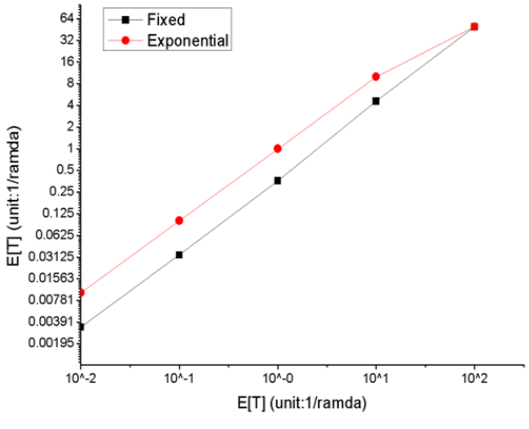


그림 8. E[t*k|tM≤tK] 그래프 비교
Fig. 8. Compare the graph E[t*k|tM≤tK]

그림 6은 E[T]의 변화에 따른 α 값의 변화를 나타낸다. 이 그래프에 따르면, α 는 E[T]에 대한 증가함수이다. 만일 E[T]가 커지면, UE가 KASME수명이 만료되기 전, oMME로 복귀할 가능성이 더 크다는 것을 알 수 있다. 또 α값은 지수분포를 T가 고정된 T보다 더 좋은 수치를 보이고 있음을 알려준다. 식(1)로부터 다음을 알 수 있다.

$$\lim_{E[T]\to\infty} \alpha = \lim_{T\to\infty}\left(\frac{e^{-\lambda T}+\lambda T-1}{\lambda T}\right)= 1 \quad (11)$$

또 $E[T]=\frac{1}{\mu}$ 일 때 식(9)를 이용하여 다음을 구할 수 있다.

$$\lim_{E[T]\to\infty} \alpha = \lim_{E[T]\to\infty}\left[\frac{\lambda}{\lambda+\left(\frac{1}{E[T]}\right)}\right]= 1 \quad (12)$$

그림 7은 미사용 키 기간인 E[tk|tM≥tk]를 E[T]에 대한 함수로 표현한 것이다. 해당 그래프를 보면, E[T]가 증가함에 따라 미사용 키 기간도 증가하고 있음을 알 수 있다. 식(2)를 이용하여, 다음 수식을 얻을 수 있다.

$$\lim_{E[T]\to\infty} E[t_K|t_M \geq t_K]$$
$$= \lim_{T\to\infty}\left(\frac{1}{\lambda}-\frac{Te^{-\lambda T}}{1-e^{-\lambda T}}\right)= \frac{1}{\lambda} \quad (13)$$

또한 $E[t_K|t_M \geq t_K]= \frac{1}{\lambda+\mu}$ 이용하여 다음의 수식을 얻을 수 있다.

$$\lim_{E[T]\to\infty} E[t_K|t_M \geq t_K]$$
$$= \lim_{E[T]\to\infty}\left[\frac{1}{\lambda+(1/E[T])}\right]= \frac{1}{\lambda} \quad (14)$$

따라서 미사용 키 기간의 최대값은 E[tM]=1/λ이며, 1/λ보다 값이 작을 때 고정 값을 가지는 T에서의 성능이 지수분포를 따르는 T에 비해 좋은 성능을 보인다. 그림 8은 재사용키 기간인 E[t*k|tM≤tk]를 E[T] 에 대한 함수로 표현한 것이다. 이 그래프에 따르면, E[T] 값이

증가함에 따라 재사용키 기간도 또한 증가한다.

식(3)을 이용하여 다음의 수식을 얻을 수 있다.

$$\lim_{E[T]\to\infty} E\left[t_K^* | t_M \le t_K\right] = \lim_{T\to\infty}\left[\frac{\lambda T^2}{2(\lambda T + e^{-\lambda T} - 1)} - \frac{1}{\lambda}\right] = \frac{1}{\lambda} \quad (15)$$

그리고 식(6)을 이용하여 다음을 구할 수 있다.

$$\lim_{E[T]\to\infty} E\left[t_K^* | t_M \le t_K\right] = \lim_{E[T]\to\infty}\left(\frac{1}{\frac{1}{E[T]}}\right) = \infty \quad (16)$$

이 그래프는 또한 T가 고정 값일 때 보다, 지수 분포를 따르는 T일 때, 재사용키 기간에 대해 더 나은 성능을 보이고 있음을 보여준다.

지금까지 구한 평균값은 개별 경우만을 고려하여 계산하였다. 따라서 KASME의 미사용 시간과 KASME의 사용기간의 두 가지 경우를 고려한 전체 평균에 대한 핸드오버 인증비용을 계산할 필요가 있다[10]. 본 논문에서는 통신 신호의 확률에 대한 평균을 구하는 공식을 이용하여 전체 평균값에 대한 각 개별 경우의 평균값을 구하였다. 이용한 공식은 다음과 같다.

$$P[signal\ present | X = K] = \frac{P[signal\ present, X = K]}{P[X = k[signal\ present]\, P[present] + P[X = k[signal\ absent]\, P[absent]} \quad (17)$$

해당 공식을 이용하여 아래 식(18),(19)를 도출하였다.

$$E[t_K | Total] = \frac{E\left[t_K | t_M \ge t_K\right]}{E\left[t_K | t_M \ge t_K\right] + E\left[t^*{}_K | t_M \le t_K\right]} \quad (18)$$

식 (18)은 KASME의 미사용 시간과 KASME의 사용기간의 두 가지 경우 중 KASME의 미사용 시간의 평균을 나타낸다.

$$E[t^*{}_K | Total] = \frac{E\left[t^*{}_K | t_M \le t_K\right]}{E\left[t_K | t_M \ge t_K\right] + E\left[t^*{}_K | t_M \le t_K\right]} \quad (19)$$

식 (19)는 KASME의 미사용 시간과 KASME의 사용기간의 두 가지 경우 중 KASME의 재사용 시간의 평균을 나타낸다.

표 5, 표6은 분석 값을 나타낸 것이며 그림 9, 그림10은 분석값을 그래프로 나타낸 것이다.

표 5. $E[t_K | Total]$

Table 5. $E[t_K | Total]$

E[T]	FIXED T	EXPONENTIAL T
$10^{-2}(\frac{1}{\lambda})$	0.6033765	0.4974874
$10^{-1}(\frac{1}{\lambda})$	0.5939961	0.4761655
$10^{0}(\frac{1}{\lambda})$	0.5378832	0.3333333
$10^{1}(\frac{1}{\lambda})$	0.1799338	0.0833332
$10^{2}(\frac{1}{\lambda})$	0.0197999	0.0196076

표 6. $E[t^*{}_K | Total]$

Table 6. $E[t^*{}_K | Total]$

E[T]	FIXED T	EXPONENTIAL T
$10^{-2}(\frac{1}{\lambda})$	0.3966234	0.5025125
$10^{-1}(\frac{1}{\lambda})$	0.4060038	0.5238344
$10^{0}(\frac{1}{\lambda})$	0.4621167	0.666666
$10^{1}(\frac{1}{\lambda})$	0.8200661	0.9166667
$10^{2}(\frac{1}{\lambda})$	0.9802	0.9803923

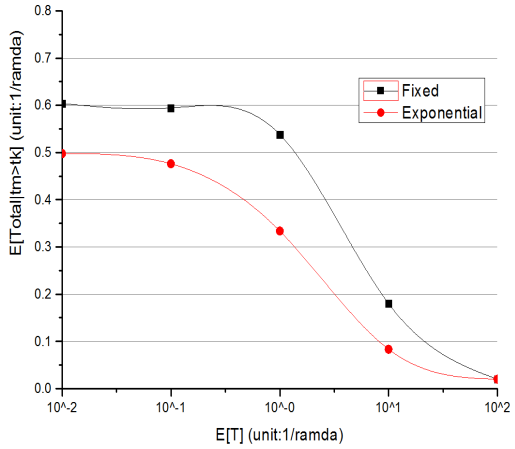


그림 9. $E[t_K|Total]$
Fig. 9. $E[t_K|Total]$

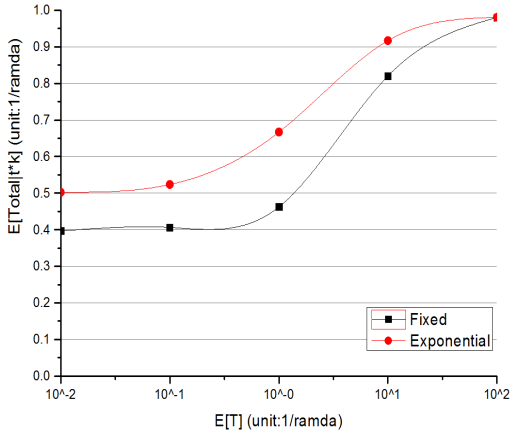


그림 10. $E[t^*_K|Total]$
Fig. 10. $E[t^*_K|Total]$

그림 9는 두 가지 경우를 고려한 전체 평균에 대한 KASME의 미사용 시간의 평균을 보여준다. E[T]가 증가함에 따라 고정된 T일 때보다 지수 분포 T 일 때 미사용 시간의 평균이 더 작으므로 지수 분포 T일 때가 더 나은 성능을 보이고 있다. 그림 10은 두 가지 경우를 고려한 전체 평균에 대한 KASME의 재사용 시간의 평균을 보여준다. 이 경우도 마찬가지로 고정된 T일 때보다 지수 분포 T일 때 재사용 시간의 평균이 더 크므로 지수 분포 T일 때가 더 나은 성능을 보이고 있다. 이 결과를 보면 대부분의 경우 지수 분포를 따르는 T에서의 성능이 고정된 T에서 보다 나은 성능을 보이고 있음을 나타낸다.

V. 결 론

본 논문은 LTE 네트워크에서의 효율적인 핸드오버를 위한 키캐싱 메카니즘을 제안하였다. 제안한 메카니즘은 UE가 oMME에서 nMME로 핸드오버 시 oMME는 UE의 KASME 을 저장한다고, 만약 UE가 KASME 의 수명이 만료 전에 oMME로 복귀한다면 UE는 oMME에 저장되어있던 KASME을 재사용하여 인증 과정을 간소화할 수 있는 기법이다. 또한 KASME의 수명에 따른 효율성을 분석하여 KASME의 저장 메모리를 낭비하지 않으면서도 효율적인 키캐싱 메카니즘을 제안하였다. 결과적으로 고정된 T값을 가질 때 보다 지수분포를 보이는 T값을 가질 때 성능이 우수한 것을 알 수 있다.

향 후 과제로는 KASME를 메모리에 저장하여 재사용함에 있어서 노출될 수 있는 보안적인 문제점에 대해서 찾아내는 것이고, 또한 보안적인 측면과 효율적인 측면 모두를 고려한 방안 제시할 필요성이 존재한다.

References

[1] 3GPP TS 36.331, “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification”
[2] 3GPP TS 36.423, “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP)
[3] 3GPP TS 36.331 V9.3.0 2010-06
[4] Long Term Evolution (LTE): A Technical Overview
[5] 3GPP TS 36.300, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description”
[6] A Key Caching Mechanism for Reducing WiMAX Authentication Cost in Handoff IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 8, OCTOBER 2009
[7] 3GPP TS 24.301, “Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3”.
[8] 3GPP TS 33.401, “3GPP System Architecture

Evolution (SAE); Security Architecture".
[9] Management Schemes in LTE Networks
[10] June-Hee Lee, Jongpil Jeong, "Performance Analysis of Cost-Effective Location and Service" JIWIT 2012-6-1, December 2012
[11] H. Yi, S. Kim, J. Choi, "Analysis of TCP Performance in LTE Wireless Network" Journal of Korean Institute of Information Technology, vol. 11, no.5, pp. 97-104, May 2013.
[12] Seo-Kwan Jeon, Soo-Hyun. oh, "An Efficient Authentication Mechanism Strengthen the Privacy Protection in 3G Network" Journal of the Korea Academia-Industrial cooperation Society, v.11, no.12, December 2010.
[13] http://www.netmanias.com/

※ 이 논문은 2013년도 한국연구재단의 재원으로 LINC사업단- LINC-URP사업의 지원과 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(NRF-2010-0024695). 교신저자 : 정종필

저자 소개

황 학 선(정회원)

• 2010 ~ : 성균관대학교 컴퓨터공학과

<주관심분야 : 모바일 네트워크, 네트워크 인증>

정 종 필(정회원)

• 2008년 : 성균관대학교 정보통신대학 (공학박사)
• 2009년 : 성균관대학교 컨버전스연구소 연구교수
• 2010년 ~ : 성균관대학교 정보통신대학 겸 산학협력단 산학협력중점교수

<주관심분야 : Mobility Management, Proxy Mobile IPv6, IEEE 802.16e, Seamless Handover, IPTV, NGN, Home Networking, IMS, Network Security>