ISSN(Print): 2287-5891

http://dx.doi.org/10.3745/KTCCS.2012.1.2.109

Reducing of Authentication Signaling Traffic in LTE Networks

Seonho Kim† · Jongpil Jeong††

ABSTRACT

As a result of the prevalence of smartphone, various mobile services became faster by LTE networks. Because many mobile devices are used more wireless services, heavy signaling traffic for authentication could be generated. Authentication is an important factor in wireless networks to identify devices; it is the start of wireless networks. This paper analyzes previous patterns for more effective authentication in accessing of another external networks. We propose a fast authentication scheme for minimizing of signaling cost between the authentication server and external networks. And we calculate the rate of authentication occurrence in LTE networks using mathematical modeling as well as the change of signaling cost for authentication in various network environments. Finally, we calculate the optimized number of authentication data and show the effectiveness for authentication signaling costs.

Keywords : LTE(Long Term Evolution) Networks, EPS(Evolved Packet System), Authentication and Key Agreement, Mobile Network Security, Poisson Distribution

LTE 네트워크에서 인증 시그널링의 감소 기법

김 선 호† · 정 종 필††

요 약

현재 많은 스마트폰의 보급으로 LTE 네트워크를 통해 다양하고 빠른 모바일 서비스를 하게 되었다. 이에 수많은 모바일 기기들이 이전보다 더 많은 무선서비스를 이용하게 되고 그에 따른 수많은 인증 시그널링이 발생하게 된다. 이러한 무선네트워크에서 인증은 무선기기를 식별할 수 있는 중요한 역할을 하며 무선네트워크의 시작이기도 하다. 그래서 본 논문에서는 이전에 인증이 발생된 패턴을 분석하여 또 다른 외부 네트워크로 접근할 때 이전 보다 효과적인 인증을 수행한다. 그래서 LTE 네트워크에서 외부 네트워크와 인증서버 사이의 시그널링 비용을 최소화하여 빠른 무선 인증 서비스를 제안한다. LTE 네트워크에서 인증이 발생되는 비율을 수학적 모델링을 이용하여 계산하였고, 이를 다양한 환경에서 인증 시그널링 비용의 변화를 계산하였다. 본 논문에서 제안한 최적 인증 데이터의 수를 계산하여 이전 보다 효율적인 인증 시그널링 비용이 발생함을 보인다.

키워드 : LTE(Long Term Evolution) 네트워크, EPS(Evolved Packet System), 인증과 키 동의, 모바일 네트워크 보안, 푸아송 분포

1. 서 론

요즘 많은 스마트 폰의 보급으로 모바일 유저들은 다양한 서비스를 사용할 수 있게 되었다. 이런 모바일의 다양한 서비스는 좀 더 빠른 무선 네트워크의 수요로 나타났고, 통신사들은 LTE(Long Term Evolution) 서비스를 가입자에게 제공하게 되었다. 3G에 비해 LTE의 주요 이점은 높은 처리량, 낮은 지연 시간, 플러그앤 플레이, 같은 플랫폼에서FDD(Frequency Division Duplex)와 TDD (Time Division Duplex)를 사용할 수 있다는 점, 향상된 사용자 성능, 단순한 아키텍쳐, 그로 인한 낮은 운영비 등이다. EPS(Evolved Packet System)는 LTE, HSDPA/HSDPA+(High Speed Downlink Packet Acess)등 다양한 액세스 네트워크를 지원하는 All-IP 기반의 시스템이다. LTE는 EPS 기술을 이용하고 이는 3GPP(3rd Gerneration Partnership Project)의 릴리즈 8을 기반하고 있으며 현재 릴리즈 10까지 나왔다[8].

하지만 빠른 무선 네트워크를 제공하는 LTE에서의 EPS 기술은 불법의 접근, 악의적인 수정, 서비스 거부 공격 등의 이전보다 많은 위험에 노출되어 있다. 그래서 3GPP는 기존의 3G망에서의 보안을 개선할 수 있는 정교한 키 계층 과 보안 컨텍스트 교환을 제공하는 새로운 보안 표준 발표했다[1]. 강화된 EPS 네트워크에서 인증의 중요성은 매우 크다.

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0027030).
† 준 회 원 : 성균관대학교 정보통신대학 정보보호학과 공학석사
†† 정 회 원 : 성균관대학교 산학협력단 산학협력중점교수
논문접수 : 2012년 6월 4일
심사완료 : 2012년 8월 7일
* Corresponding Author : Jongpil Jeong(jpjeong@skku.edu)

무선 네트워크에서 인증은 외부 네트워크에 노출된 무선기기의 익명성을 보장하면서 자신을 정보를 인증서버로부터 증명할 수 있게 한다. 이처럼 무선 네트워크에서 인증은 가장 중요한 요소이면서 가장 많이 수행되는 서비스이다. LTE는 기존 HSDPA보다 12배 이상 빠른 속도로 통신할 수 있다. 이에 더 많은 무선 네트워크 서비스를 사용하게 되었고 그에 따른 이전 보다 더 많은 인증 시그널링이 발생 하게 되었다. 하지만 3GPP의 EPS 기술에는 인증 시그널링 로드를 평가하는 연구는 없었다. 그래서 본 논문에서는 가입자의 인증 이벤트 패턴을 분석하고 그 가입자에 맞는 최소의 인증 시그널링 비용을 발생시켜 외부 네트워크와 인증서버간의 최소한의 인증 시그널링 비용을 발생시킬 수 있는 기법을 제안한다.

외부 방문 네트워크에 접근한 모바일 유저는 인증 이벤트를 발생시키고 홈 네트워크에 있는 HSS(Home Subscriber Server)로부터 인증 데이터를 요청한다. 이때 홈 네트워크에 접근비용이 비싸기 때문에 인증 서버는 한 번에 여러 개의 인증 데이터를 방문 네트워크에 전송해 준다. 본 논문에서는 외부 네트워크에서 홈 네트워크에 있는 HSS와의 접근을 최소화하여 트래픽비용을 줄이려한다. 그래서 HSS로부터 한 번에 여러 개의 인증데이터를 받아 적절한 수를 측정하여 방문 네트워크와 홈 네트워크의 접근을 최소화한다.

LTE 네트워크에서의 인증은 방문 네트워크와 홈 네트워크의 위치적인 문제점과 네트워크 방식의 차이점으로 외부 방문 네트워크와 인증서버(HSS)간의 인증 정보 요청 또는 전달에 있어 많은 네트워크 비용이 발생한다. 때문에 3GPP에서는 HSS에서 한 번에 여러 개의 인증 벡터를 보내어 외부 네트워크에서 사용할 수 있게 한다. 3GPP의 TS 29.002의 인증 정보 맵에서 3G의 인증 벡터 수는 5로 고정되어 있다[2]. 이는 LTE 네트워크의 다양한 인증 이벤트 환경에 적합하지 않다. LTE 네트워크에서는 가입자가 인증 벡터 수를 HSS에게 요청할 수 있다. 그래서 본 논문은 HSS에게 인증 벡터 수를 요청할 때 최적의 인증 벡터 수를 요청하여 특정 외부 네트워크 내에서 사용하여 HSS와 외부 네트워크 간의 트래픽을 최소화하려고 한다. 가입자가 인증을 발생시키는 비율을 다양한 수학적 모델링을 이용하여 다양한 환경에서의 인증 발생 패턴을 분석한다. 분석한 인증 발생 패턴을 기반으로 최적의 인증 벡터 수를 계산하여 최소의 인증 시그널링 비용을 발생시키도록 한다.

논문의 구성은 다음과 같다. 관련연구에서는 이전의 다양한 모바일 네트워크 인증 기법과 LTE 네트워크 시스템, LTE에서 사용하는 EPS 기술의 인증(EPS-AKA) 절차에 대해 기술했다. 그리고 제안 기법에서는 수학적 모델링을 통해 LTE에서의 인증 시그널링 비용을 수식으로 표현한다. 그 수식을 통해 본 논문에서 제안하는 기법으로 최적의 인증데이터 수를 계산하여 최소의 비용을 분석하고 증명한다.

2. 관련 연구

2.1 모바일 네트워크 인증

3GPP에서의 인증서버는 모바일 네트워크 인증과 키 동의가 발생할 때 한 번에 여러 개의 인증 벡터들을 발생시키고 방문한 외부 네트워크(visited network)에 여러 개의 인증 벡터들을 한 번에 전달한다. 이 기술은 방문한 외부 네트워크와 인증서버 사이의 많은 시그널링 트래픽을 감소시킨다. 하지만 방문한 외부 네트워크에는 그 여러 개의 인증 벡터들을 저장할 추가의 스토리지 비용이 발생하게 되었다[3][4]. 이전의 연구들에서 많은 분석 모델들은 이러한 전달되는 인증 벡터 수의 중요성을 연구하였다[5][6]. Lin은 인증 벡터들의 수를 이용하여 인증 시그널링 트래픽분석에 대한 최초의 연구를 시도했다[5]. 복잡하지 않은 알고리즘들을 통해 인증 벡터 수의 크기를 결정하여 인증 서버에 도움을 줄 수 있는 기법이 제안되었다. Al-Saraireh은 Lin의 기법은 최적의 시그널링 트래픽 감소에 대한 알고리즘을 좀 더 개선했었다[6]. Lin 과 Al-Saraireh의 분석적 모델링 방법론은 푸아송 도착 프로세스와 셀에 머무르는 시간 등에 대하여 지수 분포를 기반으로 하는 기법에서 상당히 유사하다. 한편 Zhang은 결국 이전에 사용되던 인증 벡터는 모두 사용해야지만 다음 인증 이벤트 때에 인증 서버로부터 새로운 인증 벡터를 받을 수밖에 없다는 것에 주목했다[7]. 그들이 제안한 Pre-authentication 기법은 약간 증가된 시그널링 오버헤드와 함께 인증 지연을 감소시키는 것을 보여준다. 최소한의 인증 시그널링 트래픽을 위해서는 적절한 인증 벡터 배열의 크기를 통해 최소 HSS의 접근으로 전송 비용을 줄이는 것이다. 이러한 이전의 연구들을 통해 최근의 LTE에서 사용되는 EPS기술의 인증(EPS-AKA)에 적합한 인증 시그널링 감소기법을 제안하려 한다.

2.2 LTE Networks System

LTE 네트워크에서는 3G 기술에서 발전한 다양한 요소들이 있다. Table 1에서 LTE 네트워크에서의 약어들을 명시하였고, Fig. 1은 가입자가 이동하면서 새로운 외부 네트워크에 접근하였을 때 유저 데이터의 라우팅에 대한 LTE 네트워크 시스템 및 보안 기술을 나타내었다[1][8].

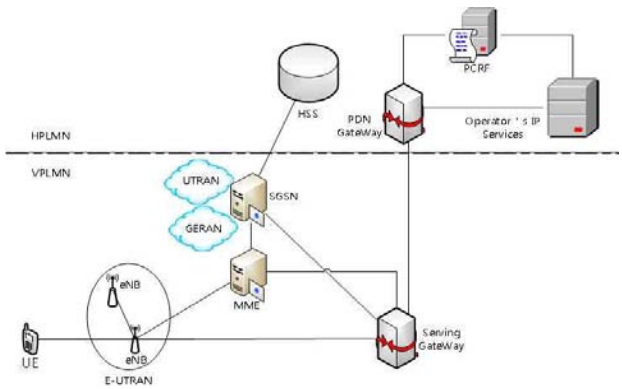


Fig. 1. LTE network system

Table 1. Acronyms for the LTE system

약어	설명
AKA	Authentication and Key Agreement
ASME	Access Security Management Entity
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
eNB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HPNMN	Home Public Land Movile Network
HSS	Home Subscriber Server
MME	Mobility Management Entity
PLMN	Pubic Land Mobile Network
RAND	RANDom number
RES	Response
UE	User Equipment
UICC	Universal IC Card
USIM	Universal Subscriber identity Module
VPLMN	Visted Public Land Mobile Network

LTE 네트워크에서 가장 중요한 세 가지 개념은 HPNMN(Home Public Land Movile Network), VPLMN (Visted Public Land Mobile Network) 그리고 UE(User Equipment)이다. 모바일 사용자는 UE로 표기 되며, UE는 ME(Mobile Equipment)와 가입자 모듈 (UICC/USIM)으로 구성되어진다.

1) HSS(Home Subscriber Server) : HSS는 UMTS (Universal Mobile Telecommunication System)의 HLR (Home Location Register)에서 발전한 것으로 홈 네트워크(HPLMN)에서 가입자 정보를 관리하는 중앙 집중화된 데이터베이스이다. HSS는 사용자의 등록/변경 관리, 인증 권한 부여, 로케이션, 세션 라우팅, 과금 등의 호/세션 제어를 위한 모든 가입자 정보를 관리한다. LTE 네트워크 시스템에서 HSS는 EPS-AV(EPS Authentication Vector) 라고 불리는 인증서를 EPS-AKA 프로토콜에 의해 MME에게 전달한다.
2) MME(Mobility Management Entity) : UMTS에서의 SGSN에서 발전한 MME는 SGSN과 마찬가지로 방문한 외부 네트워크(VPLMN)에 위치하며, EPS-AKA 프로토콜에서의 시도-응답에 대한 네트워크 종단이다. 사용자 인증과 사용자 프로파일의 다운로드를 위하여 HSS와 통신하고, NAS(Non Access Stratum) 시그널링을 통해 UE에게 EMM(EPS Mobility Management) 및 ESM(EPS Session Management)기능을 제공한다. 또한 UE는 처음 무선 네트워크에 연결을 시도할 때 MME로부터 인증을 거쳐야 한다. 인증을 통한 연결 후에도 MME는 지속적으로 인증을 요구할 수 있다. 그리고 MME는 UE의 위치를 기록하고 추적할 수 있는 이동성관리의 역할을 수행한다. MME와 UE사이의 시스템 시그널링 보안은 NAS 보안으로 가능하다. NAS 보안은 UE와 MME간의 NAS 시그널링 메시지에 대한 무결성(필수)과 암호화(선택)를 수행한다.
3) eNB(eNodeB) : eNB는 LTE에서 무선 접근 포인트이고 접근한 외부 네트워크 (VPLMN)에 속해있다. 그리고 eNB는 AS(Access Stratum) 보안의 네트워크 종단이다. eNB는 E-UTRAN안에서의 코어 네트워크 쪽으로의 통신을 보호해야 한다. AS 보안은 eNB와 UE간에 RRC(Radio Resource Control) 시그널링의 데이터 무결성(필수)과 데이터 암호화(선택)을 수행하고 사용자에서는 IP패킷에 대한 암호화(선택)를 수행한다.
4) 가입 모듈 (UICC/USIM) : UICC/USIM은 E-UTRAN의 접근하는 가입자 식별모듈이다. 이전 GSM(Global System for Mobile communications)의 SIM 스마트카드 또한 호환성의 이유로 UTRAN/UMTS로 접근이 허용되어야 하지만 GSM의 SIM은 GSM 보안과 싱글 64-bit 암호화 키(Ke) 때문에 제한되어진다. UMTS에서의 사용되는 2개의 128-bit키(CK, IK)에서 64-bit 키(Ke)로 변경하는 것은 암호학에서는 불가능한 일이기 때문에 GSM의 SIM은 E-UTRAN의 접근을 허락하지 않는다.
5) 모바일 장비(ME) : UMTS에서 ME는 오직 무선 암호에 대해서만 책임지고 있다. 하지만 LTE에서의 ME는 무선 암호뿐만 아니라 UMTS-AKA에서 발전된 EPS-AKA 프로토콜의 키 체계를 유도해야 한다.

2.3 LTE 인증 절차

UTMS과 LTE에서 인증서(Authentication Credentials)는 인증 벡터(AV)라고 한다. LTE에서는 EPS-AV라 하며, UMTS에서와는 다르게 세션 키가 K_{ASME}마스터키로 대체되었다[1]. Fig. 2는 EPS-AKA프로토콜을 이용한 EPS-AV 전달을 보여준다.

LTE에서의 인증은 네트워크에 대한 모바일의 인증뿐만 아니라 모바일에서의 네트워크 인증을 지원한다. 그래서 LTE에서 인증은 홈 네트워크의 HSS 와 UE의 USIM등 2개의 주요한 인증 프로세스가 있다. 인증 절차는 다음과 같은 두 가지 절차로 나타낼 수 있다.

- 인증 벡터 분배(Distribution of authentication Vector) : HSS가 MME에게 EPS-AV를 분배하는 절차이다.

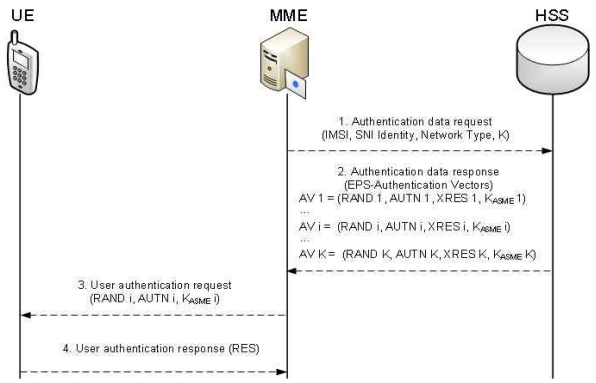


Fig. 2. LTE certification process

MME는 HSS에게 EPS-AV의 수 K를 요청하여 여러 개의 EPS-AV를 K의 수만큼 한 번에 받을 수 있다.

- 인증과 키 설정(Authentication and Key Establishment) : LTE에서 각각의 인증은 모바일과 HSS가 보안키를 공유하는 것에서부터 이루어진다. MME은 HSS로부터 EPS-AV를 분배받고 해당 보안정보를 통해 모바일에게 인증을 해줄 수 있는 것이다.

Fig. 2와 같이 LTE의 EPS-AKA 인증 절차는 다음과 같이 이루어진다[1].

1단계) UE가 새로운 MME지역으로 이동할 때, MME은 이전에 저장된 인증정보를 이용할 수 없다. 그래서 MME는 HSS에게 인증 데이터 요청메시지를 통해 인증 벡터 분배절차를 수행한다. 이 메시지는 UE의 고유한 식별 값인 IMSI(International Mobile Subscriber Identity), 가입자가 접속한 망을 나타내는 SN ID 값, 인증 벡터의 수 K, UE가 접속한 망의 종류(Networks Type)을 포함한다.

2단계) MME로부터 받은 IMSI는 HSS에 기록된 UE와 식별하기 위해 사용한다. 식별을 통해 HSS가 발생된 데이터와 인증데이터 요청정보로 HSS는 MME에게 전송할 최상위 레벨의 마스터키 K_{ASME}를 생성한다. K_{ASME}는 SN ID 값을 이용하여 생성되기 때문에 접속한 망이 바뀔 때 마다 새로운 K_{ASME} 값을 생성한다. HSS는 K_{ASME}를 이용하여 인증 벡터 AV=(RAND, AUTH, XRES, K_{ASME})를 요청한 K 수만큼 생성하여 인증 데이터 응답메시지를 통해 MME에게 보낸다. AV는 랜덤 숫자인 RAND, 예상되는 응답 값XRES, 마스터 키 K_{ASME}, 그리고 인증 토큰 AUTN으로 구성되어 있다.

3단계) MME가 UE의 인증을 시작할 때, HSS로부터 전달받은 정의된 인증 벡터 배열의 사용되지 않은 다음의 인증 벡터를 선택한다. 그리고 인증 요청 메시지를 통해 UE에게 i번째 인증 벡터 RAND i, AUTN i과 KASME i를 보낸다.

4단계) UE는 HSS에서 사용한 것과 같은 EPS-AKA 알고리즘을 통해 $AUTN_{UE}$ 값을 생성하고 AUTN i값과 비교하여 LTE망을 인증한다. 그 후에 AKA 알고리즘을 통해 발생된 RES를 인증 응답 메시지를 통해 MME에게 전달한다. MME는 받은 RES를 HSS로부터 받은 XRES와 비교한다. 만약 그들이 같다면, UE의 인증은 성공적으로 완료된다[1].

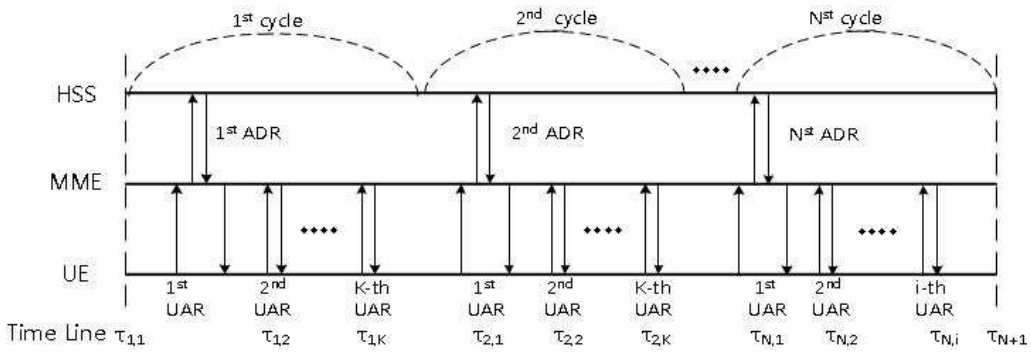
3. 제안 기법

3.1 인증 시간 다이어그램

UE가 이동하며 일어나는 인증 이벤트들을 시간 다이어그램으로 표현하고 EPS-AV 배열의 크기 K값이 인증 시그널에 미치는 영향을 알아본다. 그리고 수학적 모델링을 이용하여 EPS-AV 배열의 크기 K의 변화에 따른 인증 시그널링 비용을 산출하고 최적의 K값을 산출한다.

Fig. 3의 시간 다이어그램에서 UE가 새로운 MME 지역을 시간 $\tau_{1,1}$에 들어간다고 가정한다. UE는 MME에게 등록 메시지를 보낸다. MME가 인증정보를 가지고 있지 않기 때문에 ADR을 통해 인증 벡터를 전달받는 절차가 수행되어지고, 이때 HSS로부터 받은 인증 벡터들의 수는 K라고 한다. MME는 HSS로부터 인증 벡터 배열을 얻고 상호간의 인증은 MME와 UE/USIM 사이에 첫 번째 인증 벡터를 UAR 메시지를 통하여 사용한다[5].

시간 $\tau_{1,1}$ 후에, 두 번째 인증 이벤트는 시간 $\tau_{1,2}$에서 수행되어진다. UE/USIM의 두 번째 UAR 이벤트가 시작되어지고 MME는 상호인증에 대해 인증 벡터 배열의 두 번째 인증 벡터를 사용한다. 시간 $\tau_{1,K}$에 K번째 인증 이벤트가 수행되어 지면서 인증 벡터 배열의 K번째 인증 벡터가 UAR 메시지에 의해 사용한다. 시간 $\tau_{1,K}$ 후에는 인증 벡터 배열에 더 이상의 인증 벡터가 없으므로 다음 인증 이벤트는 시간 $\tau_{2,1}$에서 새로운 인증 배열을 요청한다. MME는 K번째 이벤트를 수행한 후 가능한 인증 벡터가 없는 것을 인식할 때, HSS로부터 다음 인증 벡터 배열을 얻기 위해 두 번째 ADR 절차가 수행되고 새로 받은 인증 벡터 배열의 인증 벡터들을 통해 다음 UAR이 수행한다. 다음 발생한 인증 이벤트들은 ADR들과 UAR들은 이미 설명했던 것처럼 반복 수행한다. 시간 τ_{n+1}때에는 UE는 MME 지역을 떠난다. 시간 τ_{n+1}이전에 마지막 인증 이벤트는 시간 $\tau_{n,i}\ (1 \le i \le k)$때에 수행되어 지며, 인증 벡터 배열에서 i번째 인증 벡터를 활용한다. 그리고 시간 τ_{n+1}에 $K-i$ 만큼의 나머지 인증 벡터 개수는 MME에서 사용 되지 않는다. 결국 τ_{n+1}~ $\tau_{1,1}$ 동안에 $(N-1)K+i$만큼의 UAR과 N번의 ADR들이 수행한다.



ADR : Authentication Data Request & Response UAR : User Authentication Request & Response

Fig. 3. Timing Diagram

MME와 HSS는 다른 지역에 위치해 있는 경우가 많다. 그래서 ADR 명령은 비용이 많이 든다는 것을 알고 있다. 그러므로 MME 지역에서 UE가 있을 때 ADR들의 수행 숫자를 감소시키기 위해 한 번에 많은 인증 벡터들을 가져와야 한다. 즉 인증 벡터 배열 크기 K는 증가되어야 한다. 하지만 큰 K값은 MME에서 HSS로부터 매번 인증 벡터들을 전송하는 동안 더 많은 네트워크 대역폭을 사용해야 한다. 이와 같이 인증 네트워크 시스널링 비용을 최소화하기 위한 적절한 K값을 선택해야만 한다. 다음 절에서는 분석적 모델을 통해 인증 시그널링 비용을 최소화할 수 있는 최적의 K 값을 계산할 수 있는 기법을 제안한다.

3.2 K값에 따른 분석 모델링

n은 UE가 한 MME 지역에 있을 때의 ADR이 수행되는 총 횟수이다. HSS로부터 얻은 각각의 ADR에 대한 인증 벡터들의 수를 K라고 한다. UE가 특정 시간동안 MME에서 일어나는 인증 이벤트를 푸아송 프로세스의 형식으로 제안하였다. 특정한 기간 τ동안 UAR은 수행된다고 하면 $\Theta(n, K, \tau)$는 HSS에서 ADR이 n번 일어날 확률이다. 만약 특정기간 τ에서 $(n-1)K + k(1 \le k \le K)$ 만큼 UAR 이벤트가 발생한다면 n번의 ADR이 수행될 것이다. 푸아송 분포의 확률에 따르면 다음과 같이 표현된다.

$$\Theta(n, K, \tau) = \sum_{k=1}^{K} \left\{ \frac{(\lambda\tau)^{(n-1)K+k}}{[(n-1)K+k]!} \right\} e^{-\lambda t} \qquad (1)$$

t는 UE가 한 MME 지역에 머무는 시간이다. Fig. 3에 의하면 $t = \tau_{N+1} - \tau_{1,1}$로 표현될 수 있다. 시간 t가 밀도함수 $f(t)$, 평균 $1/\mu$, 그리고 라플라스 변환식 $f^*(s) = \int_{t=0}^{\infty} f(t)e^{-st}dt$ 에 대한 분포를 가지고 있다고 가정한다. 다음 수식 (2)의 $P(n, K)$는 UE가 MME지역에 머무르는 동안의 ADR이 n번 일어날 확률을 나타낸다.

라플라스 변환식 방법을 이용하여 수식 (2)에서 (3)을 도출하였다. $E[N]$은 한 MME 서비스 지역에서 UE가 머무르는 동안 예상되는 ADR의 이벤트 횟수이다. 그리고 다음과 같이 나타내었다.

$$E[N] = \sum_{n=1}^{\infty} nP(n, K) \qquad (3)$$

다음과 같이 3개의 MME에 머무르는 시간 분포들을 기반으로 $P(n, K)$과 $E[N]$을 도출하였다.

감마 분포(Gamma Distribution) : 만약 $f(t)$가 평균 $1/\mu$이고 분산 υ 라면 다음과 같다.

$$f^*(s) = (1+\mu\upsilon s)^{-(1/\mu^2\upsilon)}$$

$$\frac{d^\iota f^*(s)}{ds^\iota} = (-\mu\upsilon)^\iota \left[\prod_{j=0}^{\iota-1} \left(\frac{1}{\mu^2\upsilon} + j \right) \right] (1+\mu\upsilon s)^{-(1/\mu^2\upsilon+\iota)} \qquad (4)$$

특히 감마분포의 혼합은 거의 근사치에 가까운 양수의 확률 변수를 보여준다. 또한 실제 모바일 네트워크에서 UE가 MME에 머무르는 시간을 계산할 수 있다. 때문에 각각 다른 MME에 머무르는 시간 분포를 나타나기 위해 감마 분포는 사용하기 충분하다[5].

수식 (4)와 (2)을 다시 나타내면 다음 수식(5)와 같다.

하이퍼-얼랑 분포(Hyper-Erlang Distribution) : 실수가 아닌 확률 변수의 확률 분포를 위한 매우 좋은 근사치에 가까울 수 있는 또 다른 분포는 Hyper-Erlang 분포이다. 다음과 같이 도출할 수 있다.

$$E[t] = \frac{1}{\mu} = \sum_{i=1}^{I} \left(\frac{\beta_i m_i}{\mu_i} \right)$$

여기서 m_i는 양의 정수이다.

$\beta_{i \ge 0}$ 그리고 $\sum_{i=1}^{I} \beta_i = 1$

Hyper-Erlang 분포의 라플라스 변환식으로 변환하면 다음 수식(6)과 같다.

$$\begin{aligned} P(n, K) &= \int_{t=0}^{\infty} \Theta(n, K, t) f(t) dt \\ &= \sum_{k=1}^{K} \int_{t=0}^{\infty} \left\{ \frac{(\lambda t)^{(n-1)K+k}}{[(n-1)K+k]!} \right\} e^{-\lambda t} f(t) dt \\ &= \sum_{k=1}^{K} \left\{ \frac{\lambda^{(n-1)K+k}}{[(n-1)K+k]!} \right\} \int_{t=0}^{\infty} t^{(n-1)K+k} \times f(t) e^{-\lambda t} dt \\ &= \sum_{k=1}^{K} \left\{ \frac{\lambda^{(n-1)K+k}}{[(n-1)K+k]!} \right\} (-1)^{(n-1)K+k} \times \left[\frac{d^{(n-1)K+k} f^*(s)}{ds^{(n-1)K+k}} \right] \Big|_{s=\lambda} \end{aligned} \qquad (2)$$

$$P(n,K)=\sum_{k=1}^{K}\frac{(\lambda\mu\upsilon)^{(n-1)K+k}}{[(n-1)K+k]!}\times\left\{\left[\prod_{j=0}^{(n-1)K+k-1}\left(\frac{1}{\mu^2\upsilon}+j\right)\right]\times(1+\mu\upsilon\lambda)^{-\left[1/\mu^2\upsilon+(n-1)K+k\right]}\right\} \quad (5)$$

$$f^*(s)=\sum_{i=1}^{I}\beta_i\left(1+\frac{s}{m_i\mu_i}\right)^{m_i} \quad (6)$$

$$P(n,K)=\sum_{i=1}^{I}\beta_i\left\{\left[\frac{(m_{i-1})!\mu_i^{m_i}(m_{i\lambda})^{(n-1)K}}{(m_i\lambda+\mu_i)^{(n-1)K+m_i}}\right]\times\left[\sum_{k=1}^{K}\left(\frac{(n-1)K+k+m_i-1}{m_i-1}\right)\left(\frac{m_i\lambda}{m_i\lambda+\mu_i}\right)^k\right]\right\} \quad (7)$$

여기서 수식 (6), (2)을 다시 쓰면 다음 수식(7)과 같다.

지수 분포(Exponential Distribution) : 수식 (5)에서 $\mu^2\upsilon=1$거나 (7)에서 $I=1,\ m_i=1$ 라고 할 경우, t는 지수 분포를 이용하여 수식 (2)를 다음과 같이 나타낼 수 있다.

$$P(n,K)=\left(\frac{\lambda}{\lambda+\mu}\right)^{(n-1)K}\left[1-\left(\frac{\lambda}{\lambda+\mu}\right)\right]$$

또한 (3)도 다음과 같이 나타낼 수 있다.

$$E[N]=\frac{1}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^K} \quad (8)$$

지수 분포는 모바일 네트워크에서 MME가 머무르는 실제 시간을 상세히 계산할 수 없다. 그러나 이 분포는 평균값 분석에 대해 결과가 정확하고, 시스템의 성능 추정할 수 있다[5].

$C(K)$는 한 MME 지역에서 UE가 머무를 때 ADR들의 총 메시지 전송 비용을 나타낸다. 그리고 다음과 같이 나타낼 수 있다.

$$C(K)=E[N]\times(K+2\alpha) \quad (9)$$

여기서 α는 인증 절차를 통해 발생되는 인증 벡터 전송 비용과 인증 벡터가 발생되는 시간에 대한 정규화된 하나의 시그널링 메시지 오버헤드에 대한 비용을 나타내었다. 이 오버헤드는 하나의 ADR에서 요청과 응답 메시지를 한 쌍으로 교환 하도록 고려되어 졌다. 수식 (8)와 (9)로부터 MME에 머무르는 시간을 지수로 나타낸 것에 대한 총 ADR 비용을 다음과 같이 나타내었다.

$$C(K)=\frac{K+2\alpha}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^K} \quad (10)$$

다음의 성능평가에서 위에서 언급한 수학적 모델링을 그래프로 나타내어 다양한 K값과 UE가 MME에 머무르는 시간 분포 변화에 대한 인증 시그널링 비용을 비교해 본다. 또한 이전 MME 서비스 지역에서의 UE의 행동 패턴을 분석하여 인증 벡터 배열 크기인 최적의 K을 계산할 수 있도록 한다. 이러한 최적의 K값은 MME 서비스 지역을 이동할 때 마다 최적의 K값을 계산하여 매번 최적화된 인증 시그널링 비용을 나타낼 수 있게 된다.

4. 성능평가

4.1 K값에 따른 인증 시그널링 비용

이 단락에서는 이전의 수학적 모델링을 통해 인증 벡터 배열 크기 K값에 대한 예상되는 $E[N]$ 값과 비용 $C(K)$ 값 영향에 대해 보여준다. 인증 벡터 배열 크기 K값은 MME가 HSS에게 요청 메시지를 보낼 때 그 크기에 대한 값을 보내고 HSS는 MME가 요청한 수만큼의 인증 벡터들을 보내준다. 이전 단락에서의 분석 모델링은 특정 K값에 대한 $E[N]$과 $C(K)$을 계산할 수 있다. Table 2는 성능평가에서 사용된 변수 값이다.

Table 2. Table for calculating the variable signaling costs

Variables	Contents
K	Size of authentication vector array
k	The rest number of authentication vectors used before MME's service area leaving $(1 \le k \le K)$
n	The number of ADR
M	The total number of UAR
$\lambda(\lambda=1/\mu)$	Various UAR (authentication events) occurrence rate
$C(K)$	Total message transmission cost for ADRs when an UE resides in an MME area
$E[N]$	The expected number of ADRs when the MS resides in an MME service area
$P(n,K)$	The probability that there are n ADRs during the UEs residence in the MME area
$L(K)$	The discarded authentication vector K number(loss) in an MME service area leaving.

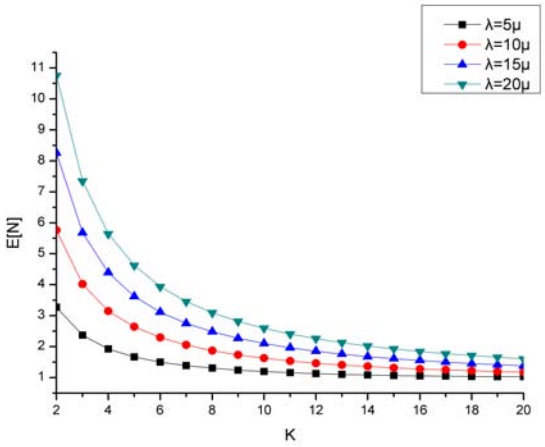


Fig. 4. Effect of UAR occurrence rate λ

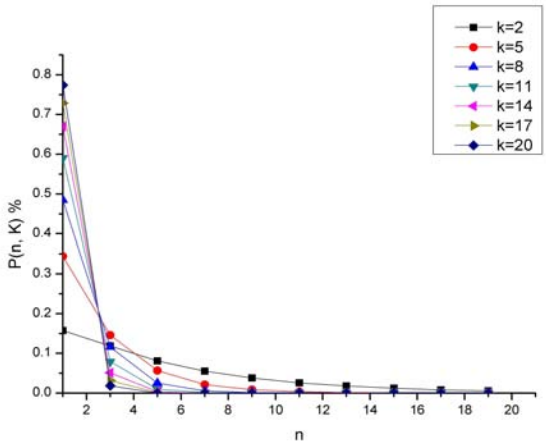


Fig. 5. The probability that ADR occurs n times

Fig. 4는 다양한 UAR(인증 이벤트) 발생 비율 λ와 K값에 대한 $E[N]$의 그래프이다. MME에서 머무르는 시간들은 평균 $1/\mu$ 의 지수적인 분포로 추정한다. Fig. 4에서 보듯이 K값이 10보다 작을 때 UAR의 발생비율이 작을수록 ADR이 일어나는 횟수가 크게 차이나는 것을 볼 수 있다. 또한 K값이 10보다 클때 5μ와 20μ 사이의 ADR이 일어나는 횟수 $E[N]$값은 많은 차이가 없다. 인증 시그널링 비용을 최소화하기 위해서는 홈 네트워크에 접근해야하는 ADR(Authentication Data Request & Response)은 최소화해야 한다. Fig. 4의 그래프는 UAR 발생 비율과 K값에 변화에 따른 시그널링 비용을 나타내고 있다.

Fig. 5 그래프는 $P(n,K)$의 확률 분포이며, 여기서 $\lambda = 10\mu$이다. $P(n,K)$는 특정 K값에 대한 ADR이 n번 발생할 확률에 대한 그래프이다. 그래프에서 $P(n,K)$ 분포는 K가 11이상이고 ADR의 횟수 n이 8이상일 때 거의 유사하며, K가 8 이하일 때 매우 다른 것을 확인할 수 있다. 특히 ADR이 3 이하로 발생할 확률에서 K값 2와 20의 차이는 매우 크다. 이것은 Fig. 4와 유사한 결과를 가지고 있다. $P(n,K)$과 마찬가지로 $E[N]$값은 큰 K값에 대한 결과가 유사하고 이는 K값의 증가는 시그널링 비용을 개선시키지 못한다는 의미이다.

Fig. 3에서 $(n-1)K+k(1 \le k \le K)$ 만큼 UAR 이벤트가 일어난다고 가정한다. 이중에서 $K-k$값은 쓸 수없는 인증 벡터로 버려지게 된다. 이는 새로운 MME 지역으로 이동할 때 이전의 MME에서 쓰다가 남은 인증 벡터를 쓸 수 없기 때문이다. 만약 매번 ADR 이벤트가 발생함에 따라 일정의 손실이 발생한다면, 그 손실은 계속해서 누적되어 전체 네트워크 트래픽에서는 많은 영향을 미치게 된다. 때문에 전체적인 네트워크 트래픽을 보았을 때에는 버려지는 인증 벡터의 손실은 크게 보인다. 그렇기 때문에 UAR 발생에 따른 네트워크 트래픽 손실 여부를 간과할 수 없다. 나머지 버려지는 인증 벡터의 손실 값은 다음과 같이 나타낼 수 있다. 여기서 k는 $1 \le k \le K$ 이고 L은 한 MME 지역에서 n번의 ADR이 발생 했을 때의 손실 값이다.

$$nK-(n-1)K+k = K-k = L(K) \qquad (11)$$

그리고 다음과 같이 UAR 이벤트 총 횟수를 M이라 할 때 다음과 같이 나타낼 수 있다.

$$M = (n-1)K + k$$
$$M \equiv L \bmod K$$

여기서 총 UAR 이벤트 횟수 M=5, M=10, M=15, M=20이라 하고 K값 변동에 따른 손실 값 L을 나타내었다. Fig. 6에서는 UAR 횟수 대비 K값 증가에 따른 네트워크 손실 값 $L(K)$을 그래프로 그렸다. 그래프와 같이 손실 값은 일정하게 증가하기 보다는 일정의 변동 폭이 있다. 다음과 같이 UAR 횟수에 따른 서로 다른 최소의 손실을 나타내고 있고 K값의 증가에 따라 더 많은 손실 변동이 발생 되었다. 이런 인증 벡터 손실을 네트워크 비용으로 생각한다면 Fig. 6 역시 K의 증가는 오히려 네트워크의 비용을 더 증가시키고 있다. 따라서 UAR 이벤트 수에 따라 최적의 K값과 인증 시그널링 비용에 영향을 주게 된다.

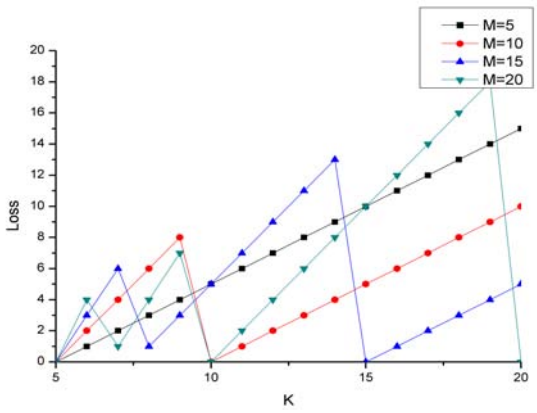


Fig. 6. For all UAR, Loss depends on changes in K values

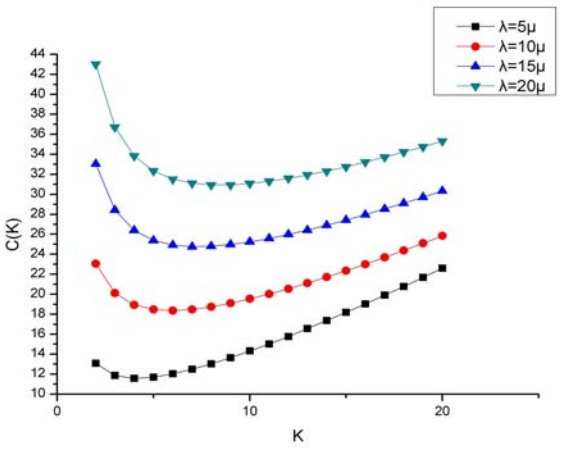


Fig. 7. The graph for $C(K)$ as a function of UAR rates

Fig. 7은 수식 (10)에서 $\alpha = 1$ 일 때, 다양한 UAR 발생 비율 λ의 K에 대한 $C(K)$값에 대한 그래프이다. 이는 MME에서 머무르는 시간은 지수분포를 이용하였고 K값이 증가할 때 $C(K)$의 값에 대한 변동을 보여 주고 있다. 최소 비용 $C(K)$에 대해 적절한 K값을 도출하기 위함이다. 또한 Fig. 7는 K값의 증가와 UAR이 발생될 비율 λ의 증가는 시그널링 비용 $C(K)$의 증가를 가져왔다. 그 결과 UAR이 발생될 비율 λ의 증가에 따른 그래프들은 K값에 대한 변동에 대해 $C(K)$가 영향을 받음을 알 수 있다. 따라서 MME가 머무르는 시간 분포는 최소의 비용을 위한 인증 벡터 배열 크기 값 K에 많은 영향을 준다.

4.2 최적의 인증 벡터 배열 크기

3GPP TS 29.002에서의 3G의 인증 벡터 배열값이 $K=5$로 모바일 기술 맵에 설정되어 있다[2]. 하지만 인증 벡터 배열 값이 고정적으로 되어있는 것은 효율적이지 못하다. 이전 성능 평가에서 UAR 트래픽에 따라 가장 최적의 K값이 변화가 있는 것이 확인하였다. 따라서 UE의 UAR 트래픽 패턴 기반으로 K값을 동적인 선택을 할 수 있는 기법을 제안한다. 이 기법은 HSS 또는 UE에서 실행되어 질 수 있다. 만약 이 기법이 UE에서 수행된다면, UE가 매번 새로운 MME 지역에 이동할 때 마다 새로운 K값 등록절차에 의해 최적의 K값을 찾도록 수행되어 질 것이다. 그리고 UE가 이전 MME지역으로 부터 이동하여 새로운 MME 서비스 지역 이동할 때 이전의 UE의 행동 패턴을 분석하여 최적의 K값을 찾고, 이를 HSS에게 요청 하며 요청한 K값 만큼의 인증 벡터 배열을 전달해 주게 된다[1]. 최적의 인증 벡터 배열 크기 K는 j번째 새로운 MME 지역에서 UE가 머무르면서 K값을 측정하여 $j+1$번째에 요청한다고 하자. 이때 최적의 K값 측정은 다음과 같이 나타낼 수 있다.

측정 단계 : j번째 MME 서비스 지역에 머무르는 동안 UAR의 이벤트 횟수 M을 측정한다.

결정 단계 : UE가 j번째 MME에 떠날 때, K값의 크기를 결정한다. 우리는 수식 (9)처럼 다음과 같은 계산방법을 따른다. L_i는 수식 (11)을 따르며 이전에서 언급했던 인증 벡터의 인증 벡터 손실을 시그널링 비용에 포함 시킨다. 인증 벡터 손실은 K값에 따라 ADR이 발생 한 만큼 증가하여 전체 네트워크 트래픽에 영향을 미칠 수 있기 때문에 인증 시그널링 비용에 포함되어야 한다. 결정단계 시 그 수식은 다음과 같이 표현된다.

$$
\begin{aligned}
K_1 &= K(j) - 2,\\
K_2 &= K(j) - 1,\\
K_3 &= K(j),\\
K_4 &= K(j) + 1,\\
K_5 &= K(j) + 2
\end{aligned}
$$

$$
c_i = \left\lceil \frac{M}{K_i} \right\rceil \times K_i + L_i(nK_i - M), \text{ for } i = 1,2,3,4,5 \tag{12}
$$

$$
K(j+1) = K_m \text{ where } 1 \le m \le 5 \text{ and } c_m = \min_{1 \le i \le 5} c_i \tag{13}
$$

수식 (12)를 통해 수식 (13)처럼 최소의 c_i값을 가지는 최적의 K_m 값을 도출 해 낸다. $j+1$번째 MME 지역을 UE가 방문했을 때 수식 (13)에서 측정 된 최적의 K_m값을 통해 HSS에게 인증 벡터 배열 크기를 요청한다. 그리고 HSS는 요청 받은 K만큼의 인증 벡터를 전달한다.

Fig. 8에서 MME에 머무르는 지수 분포는 $\lambda = 10\mu$ 이고, $K(j)$는 이전의 인증 벡터 배열의 크기이다. 여기서 old_MME는 이전에 방문 했던 MME 서비스 지역이고 new_MME는 old_MME 이후에 방문된 MME 서비스 지역이다. 그리고 $K(j+1)$은 수식 (12)과 (13)을 통해 얻어진 최적의 K값으로 계산된 인증 시그널링 비용이다. 인증 시그

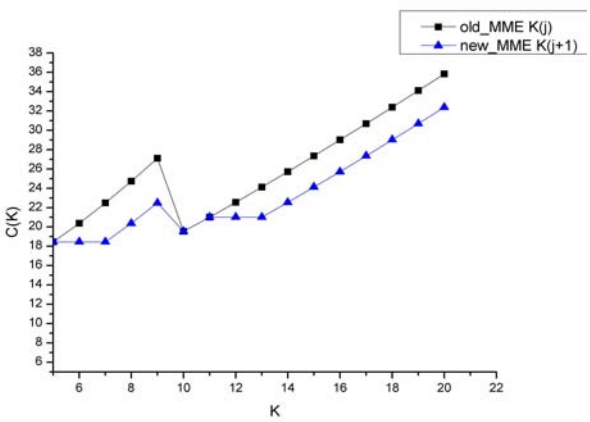


Fig. 8. Effect of reducing signaling cost as a function of K

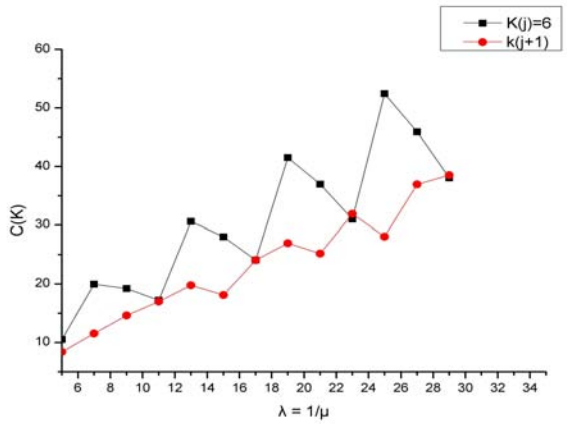


Fig. 9. Cost for optimal K as a function of UAR occurrence rate λ

널링 비용은 Fig. 8과 Fig. 9에서도 마찬 가지로 이전의 수식 (10)에서 (11)의 인증 벡터 손실 값을 더하여 시그널비용을 계산하였다. Fig. 8에서 보듯이 새로운 MME 서비스 지역을 방문하여 사용된 최적의 $K(j+1)$가 시그널 비용을 감소시킬 수 있는 것을 확인할 수 있다. 그래프 중간의 K값이 5, 10의 경우 이전과 같은 시그널 비용을 나타내고 있다. 이는 이전의 K값이 이미 최적의 비용을 나타내므로 K값을 변경할 필요가 없음을 나타낸다.

Fig. 9은 인증 벡터 배열 크기를 6으로 고정한 환경에서 지수 분포 변화에 따른 시그널링 비용을 나타내었다. 그리고 각각의 K값에 따라 최적의 K값을 계산하여 그에 따른 비용을 비교하여 나타내었다. Fig. 8과 마찬가지로 최적의 K값 계산으로 최소의 비용을 나타내고 있다. 또한 Table 3에서 보듯이 K값이 λ의 증가에 따라 계속 증가 또는 감소되지 않는 것을 확인할 수 있다.

이와 같은 성능평과들은 최적화한 K값의 선택이 최소의 인증 시그널링 비용을 가질 수 있음을 나타내고 있다. 그리고 최소의 K값을 찾기 위해서는 이전의 UE의 UAR 발생

Table 3. Change of K for a given UAR occurrence rate λ

λ=1/μ	$K(j)$	old_Cost	$K(j+1)$	new_Cost
5	6	10.5247	5	8.359491
7	6	19.95629	7	11.52635
9	6	19.20782	5	14.65165
11	6	17.21138	4	17.01067
13	6	30.64492	7	19.7658
15	6	28.03163	5	18.12885
17	6	24.11076	6	24.11076
19	6	41.52382	4	26.95508
21	6	36.95324	7	25.18574
23	6	31.06132	4	31.94145
25	6	52.45948	5	28.07837
27	6	45.909	4	36.93182
29	6	38.03191	5	38.48128

비율과 인증 벡터의 손실에 많은 영향을 받는 것을 확인하였다. 따라서 본 논문에서 제안한 최적의 K값 측정 및 결정으로 최소의 인증 시그널링 비용을 나타낼 수 있다.

5. 결 론

모바일 네트워크에서 인증은 MME 서비스 지역을 이동하거나 매 인증 이벤트들 발생할 때 수행하게 된다. LTE 네트워크에서 각각의 인증은 MME와 UE에서 수행되며, 그 인증은 HSS로부터 MME가 전달받아 인증 데이터를 얻는다. 이때, MME가 HSS에 접근하는 비용이 비싸기 때문에 접근 수를 줄이기 위해 MME는 한 번에 많은 크기의 인증 벡터를 얻어야 한다. 하지만 인증 벡터 배열에 대한 K의 크기가 커지면, 즉 한 번에 많은 인증 벡터를 전달한다면 매번 HSS에서 MME의 인증 벡터 배열 전송 비용이 더 비싸지게 된다. 또한 하나의 MME 서비스 지역이 종료되었을 때 인증 벡터 배열의 크기가 커질수록 버려지는 인증 벡터들의 수도 커져서 시그널링 비용의 낭비를 초래할 수 있다. 때문에 최소한의 인증 시그널링 비용을 위해 적절한 K값을 선택해야 한다. 여기서 제안한 분석 모델을 통하여 다음의 결과를 확인하였다.

- K값의 증가는 HSS에서 MME로부터 접근하는 횟수 $E[N]$을 감소시킨다. 그러나 K가 커질 때 증가된 K는 오직 $E[N]$의 감소만을 나타내었고 인증 시그널링 비용을 감소시키지는 못하였다.
- UE가 MME 서비스 지역에 머무르는 시간이 증가할 때 $E[N]$은 증가한다. 그만큼의 인증 횟수가 증가하면서 HSS로부터 인증 요청 횟수 $E[N]$도 증가하게 된다.
- 한 MME 서비스 지역에서 버려지는 인증 벡터의 시그널링 손실은 인증 시그널링의 증가를 가져 온다.
- UE의 인증 이벤트 패턴에 맞는 적절한 K값은 인증 시그널링 비용의 감소를 나타낸다.

인증 벡터 배열 크기 K을 조정하여 인증 트래픽의 값 $C(K)$을 줄여야 한다. 제안한 MME가 머무르는 시간 분포와 UE의 UAR 트래픽 패턴, 인증 벡터의 손실을 기반으로 한 동적인 K값을 선택하는 기법을 제안한다. 적절한 K값은 네트워크 시그널링 비용을 감소시키는데 상당히 효과적이라는 것을 보여준다. 누적된 네트워크의 전체 시그널링에 비용에서 본다면 그 효과는 더욱더 효과적일 것이다. 본 논문에서는 적절한 K값에 대해 이전의 K값과 개선된 K값의 성능 결과를 비교하여 보여준다.

참 고 문 헌

[1] Third Gerneration Partnership Project; Technical Specification Group Services and System Aspects. 3GPP System

Achitecture Evolution(SAE), “Security Architecure Security (Release 10),” 3GPP TS 33.401 version 10.2.0 September, 2011.
[2] Third Gerneration Partnership Project; Technical Specification Group Services and System Aspects. “Mobile Application Part (MAP) specification (Release 10),” 3GPP TS 29.002 version 10.6.0 March, 2012.
[3] Chung-Ming Huang and Jian-Wei Li, “Authentication and key agreement protocol for UMTS with low bandwidth consumption,” Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA), March, 2005.
[4] Ja'afer Al-Saraireh and Sufian Yousef, “A new authentication protocol for UMTS mobile networks,” EURASIP Journal on Wireless Communications and Networking, Vol.2006, Issue 2, April, 2006.
[5] Yi-Bing Lin and Yuan-Kai Chen, “Reducing authentication signaling traffic in third-Generation mobile network,” IEEE Transactions on Wireless Communications, Vol.2, No.3, May, 2003.
[6] Ja'afer Al-Saraireh and Sufian Yousef, “Analytical model for authentication transmission overhead between entities in mobile networks,” Elsevier Computer Communications, Vol.30, Issue 8, June, 2007.
[7] Yan Zhang and Masayuki Fujise, “An improvement for authentication protocol in third-generation wireless networks,” IEEE Transactions on Wireless Communications, Vol.5, No.9, September, 2006.
[8] Third Gerneration Partnership Project; Technical Specification Group Services and System Aspects. “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network(E-UTRAN) access, (Release 10),“ 3GPP TS 23.401 version 10.7.0 March, 2012.
[9] Yi-Bing Lin, Wei-Ru Lai, and Rong-Jaye Chen, “Performance analysis for dual band PCS networks,” IEEE Trans. Comput., Vol.49, pp.148-159, Feb., 2000.
[10] Koien, G.M., “Mutual Entity Authentication for LTE,” IEEE Trans Comput, pp.689-694, July, 2011.
[11] E. J. Watson, Laplace Transforms and Applications. Cambridge, MA

김 선 호
e-mail : pero5@skku.edu
2009년 안양대학교 디지털미디어공학 (공학사)
2011년~현 재 성균관대학교 정보통신대학원 정보보호학과 공학석사
관심분야 : 암호학, 인증과 키 동의, 모바일 네트워크

정 종 필
e-mail : jpjeong@skku.edu
2008년 성균관대학교 정보통신대학 (공학박사)
2009년 성균관대학교 컨버전스연구소 연구교수
2010년~현 재 성균관대학교 산학협력단 산학협력중점교수
관심분야 : 모바일 컴퓨팅, 센서 이동성, 차량 모바일 네트워크, 스마트기기 보안, 네트워크 보안, IT 융합, 인터랙션 사이언스 등