情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

3GPP LTE/SAE 네트워크에서의 인증 시그널링 부하에 대한 평가

강 성 용,[1†] 한 찬 규,[2] 최 형 기[1‡]
[1]성균관대학교, [2]삼성전자

Evaluation of Authentication Signaling Load in 3GPP LTE/SAE Networks

Seong-Yong Kang,[1†] Chan-Kyu Han,[2] Hyoung-Kee Choi[1‡]
[1]Sungkyunkwan University, [2]Samsung Electronics

요 약

통합된 코어 망 구조(core network architecture)와 다양한 무선 가입자 행동들은 3GPP in Release 8에서 제안된 EPC(Evolved Packet Core Network)에서 상당한 시그널링 부하 증가를 가져온다. 따라서 인증 시그널링 분석(authentication signaling analysis)은 체감품질(quality-of-experience)을 충족시키면서 인증 시그널링 부하와 지연을 줄이는 통찰력을 갖게 해준다. 본 논문에서는 갱신 과정 이론(renewal process theory)에 기반을 둔 분석적 모델링을 통해 EPS 구조에서의 시그널링 부하에 대해 평가하였다. 갱신 과정 이론은 특정 랜덤 과정(random process)에 상관없이 잘 작동 한다 (예. 포아송(Poisson)). 본 논문은 발신 발생 속도(call arrival rate), 이동성(mobility), 가입자들의 선호도와 운영정책의 관점에서 가입자들의 다양한 패턴을 고려하였다. 매개변수들과 성능지표들 사이의 상호관계를 나타내기 위해 수치적인 결과를 사용하였다. 수직적 핸드오버(vertical handover) 성능의 민감도와 heavy-tail process의 영향에 대해서도 검토하였다.

ABSTRACT

The integrated core network architecture and various mobile subscriber behavior can result in a significant increase of signaling load inside the evolved packet core network proposed by 3GPP in Release 8. Consequently, an authentication signaling analysis can provide insights into reducing the authentication signaling loads and latency, satisfying the quality-of-experience. In this paper, we evaluate the signaling loads in the EPS architecture via analytical modeling based on the renewal process theory. The renewal process theory works well, irrespective of a specific random process (i.e. Poisson). This paper considers various subscribers patterns in terms of call arrival rate, mobility, subscriber's preference and operational policy. Numerical results are illustrated to show the interactions between the parameters and the performance metrics. The sensitivity of vertical handover performance and the effects of heavy-tail process are also discussed.

Keywords: 3GPP authentication and key agreement (AKA), long term evolution (LTE), evolved packet system (EPS), renewal process theory, mobile network security, performance evaluation

접수일(2011년 5월 2일), 수정일(1차: 2011년 12월 18일, 2차: 2012년 2월 22일), 게재확정일(2012년 3월 23일)

† 강성용, sykang@ece.skku.ac.kr
‡ 최형기, hkchoi@ece.skku.ac.kr

I. 서 론

적은 양의 무선 자원과 고객의 수를 늘리기 위한 열망은 이동통신 시스템을 3G 무선 시스템에서 이종의 네트워크와 융합서비스로 결합된 4G 네트워크로의 진화를 위한 원동력이 되고 있다. 3GPP LTE/SAE (long term evaluation/system architecture evolution)는 더 높은 대역폭, 더 넓은 적용범위, All-IP 구조에서 이종의 시스템들이 완벽하게 상호작용 하도록 돕기 위해 EPS in Release 8에서 제안되었다. EPS 구조는 불법적인 접근, 악의적인 변조, 임의 조작, 서비스거부 등의 위험에 노출되어 있다. 따라서 3GPP는 [1]에서 발전된 더 정교한 키 구조와 보안 문맥 교환을 지원하는 새로운 보안 표준[12]을 발표하였다. 그동안, Release 5에서는 IP기반의 코어 망을 정의하기 위해 IMS(Internet Protocol Multimedia Subsystem)를 발표하였다. 하지만 IMS의 발표는 시그널링 평면의 복잡도를 더 증가시킨다[10]. 이것은 아래의 이유들 때문이다: (1) Release 5의 시그널링 프로세스는 Release 99에 비해 더 많은 네트워크 구성요소에 의해 관리된다; (2) IMS에서의 시그널링은 Release 9의 SS7보다 메시지의 크기와 계산 복잡도가 더 큰 SIP(Session Initiation Protocol)에 기반한다. 따라서 정확한 인증 시그널링 분석은 인증 시그널링에서의 부하와 지연을 줄이는 통찰력을 갖게 해준다.

Release 5이후의(EPS 포함) 3가지 특성은 아래와 같다: (1) 오직 회선 기반의 음성 서비스(예. 전화)만이 가능했던 과거와 달리 다양한 패킷 데이터 서비스(예. 인스턴트 메시징, 멀티미디어 스트리밍, 모바일 게임, 모바일 인터넷등)들이 연관되어 있다; (2) 다중 접속 네트워크가 EPS구조로 합쳐질 수 있다. 따라서 네트워크를 교차하는 핸드오버가 빈번해진다; (3) 키 계층과 조작법의 변화로 인해 인증과 키 동의 시스템이 재고되어야 한다. 지금까지 3GPP Release 8의 EPS 구조에서의 인증 시그널링 부하에 대한 평가에 관련된 연구는 없었다. 본 논문은 다양한 인증 시도 과정과 가입자의 패턴과 운영정책에 관련된 인증 시그널링 트래픽 평가를 위한 분석적 틀을 소개한다. 우리는 대기상태에서 지체하는 시간에 따라 정규화된 인증 시그널링 부하를 분석하기 위해 갱신 보상 이론(renewal reward theorem)을 적용하였다. 이전의 연구에서는 간소함을 위해 인증 요청에 대해 포아송 과정(poisson process)이 가정되었다. 그러나 busy-line effect 때문에 포아송 도착 과정(poisson call arrival process)은 적절하지 못하다[6].

본 논문의 주 관심사는 4가지로 구성되어 있다: (1) EPS와 Release 8에서 개정된 보안 구조에 대해서 소개한다; (2) 인증 요청 시도 프로세스에서의 포아송 가정(poisson assumtion)을 완화 한다; (3) 발신 시도나 위치갱신 이외에 새로운 인증 계기에 대해서 알아본다(예. 수평적 혹은 수직적 핸드오버); (4) 인증 시그널링 비용을 기점과 설명에 따라 구분한다.

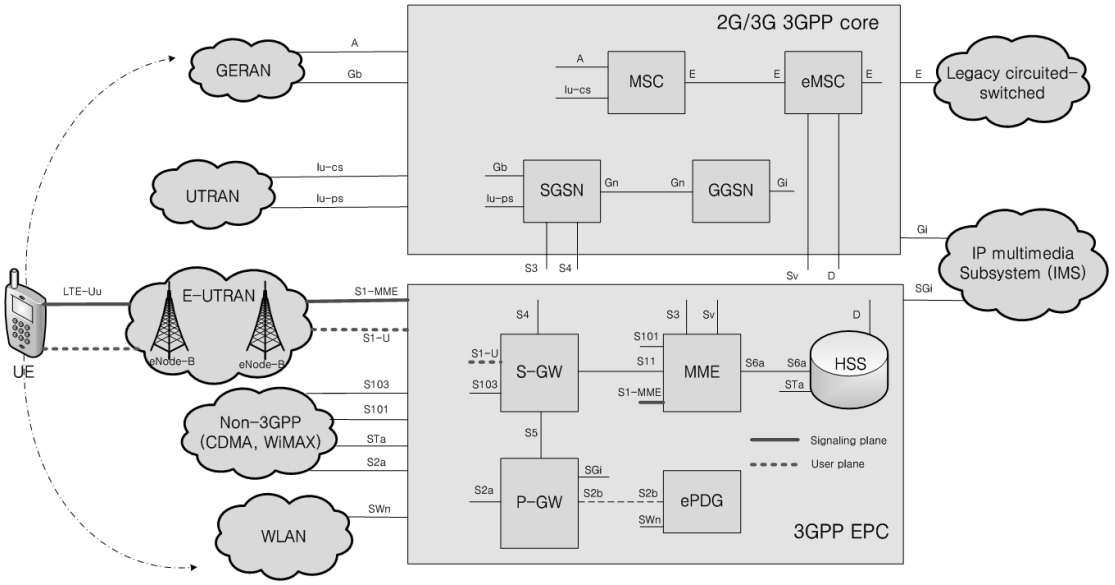
우리의 분석결과에 따르면 인증 벡터의 수 또는 암호화 키의 수명(lifetime)이 증가하면 총 신호비용 함수는 볼록한 형태를 나타낸다. 인증 서버에게 질의하는 통신지연 증가의 영향은 그다지 중요하지 않지만 인증 시도 속도의 증가는 시그널링 부하의 뚜렷한 증가를 만든다. 다른 랜덤 과정(random process)을 갖는 다양한 인증에 대해 조사하고, Erlang 분포, 초지수분포(hyper-exponential distribution), 그리고 heavy-tail 특성으로 인해 멀티미디어 처리에 적합한 Pareto 분포와 log2-normal분포에 대해서 알아보았다. 그 결과 과소평가된 Pareto가 없는 기준선 분포를 보였다. 마지막으로, 3GPP Release 8에서 새롭게 제안된 기법인 키 재사용 방법에 대해서 조사한다.

나머지 부분의 구성은 아래와 같다. 2장에서 인증 시그널링 트래픽 부하에 관련된 연구에 대해서 알아본다. 3장은 EPS 구조와 인증 절차 그리고 다양한 핸드오버 시나리오에 대해서 설명한다. 4장에서는 갱신 과정 이론을 통해 EPS의 성능에 대해 연구하기 위해 제안된 분석적 틀에 대해서 소개한다. EPS 인증과 키 동의에 대한 보안과 성능의 다양한 수치상의 분석에 대해서 5장에서 설명한다. 마지막으로 6장에서 차후 연구에 대한 소개와 함께 결론에 대해 기술한다.

II. 관련연구

3GPP 모바일 네트워크의 인증과 키 동의에서, 인증 서버는 다수의 인증 벡터를 생성하고 방문 네트워크에게 전송한다. 이러한 방법은 인증 서버와 방문 네트워크간의 시그널링 트래픽을 줄인다. 반면 이러한 방법은 방문 네트워크에게 추가적인 저장장소의 오버헤드를 갖도록 한다.

인증 벡터 수의 효과에 대해 조사하기 위해 많은 분



〔그림 1〕 SAE/LTE 시스템 구조와 EPC 네트워크 원소

석 모델이 제안되었다〔4〕〔8〕. 〔5〕에서는 새로운 인증 벡터의 대기 확률, 〔7〕에서는 사용되지 않은 인증 벡터를 관리하기 위해 필요한 시간 주기가 고려되었다. Yi-Bing Lin 등은 인증 시그널링 트래픽을 인증벡터의 수에 관하여 분석하는 선구적인 연구를 하였다. 인증 서버를 돕는 인증벡터의 수를 결정하는 매우 단순한 알고리즘 역시 제안되었다. Ja′afer Al-Saraireh 등은 시그널링 트래픽을 줄이는 알고리즘이 최적화 되어야 한다고 지적하여 Lin의 방법을 향상 시켰다〔8〕. Lin과 Al-Saraireh의 분석적인 모델링 방법은 그들이 포아송 도착 과정과 지수적인 셀 지체시간에 기초하였다는 점에서 매우 비슷하다. Yang Zhang은 모든 인증 벡터가 다 사용되고 난 후의 인증 시도는 인증 서버로 부터 인증 벡터를 가져올 때까지 기다려야만 한다고 지적하였다〔5〕. 저자는 그들이 제안한 선행-인증 방법이 적은 양의 신호증가 오버헤드를 가지고 인증 지연을 줄임을 보였다. 남아있는 인증 벡터를 관리하기 위한 적절한 저장 시간제한(timeout)이 〔7〕에서 연구되었다. 여기서는 긴 저장 시간제한 주기는 방문 네트워크의 추가적인 저장 공간 비용의 오버헤드를 갖도록 하면서 인증서버에 접속을 줄인다고 결론지었다.

이전의 연구에서는 간소함을 위해 인증 요청에 대해 〔6〕을 제외한 나머지에서 포아송 과정이 가정되었다. 최근 Yang Zhang은 〔6〕에서 다른 이동성 모델(mobility models)과 포아송 도착 과정이 아닌 다양한 랜덤 도착 과정(random arrival process)의 영향에 대해 고려하였다. 그러나 간소함을 위해 결집 도착 과정(aggregated arrival process)이 가정되었다. 이러한 가정은 다양한 형태의 인증 요청 시도 처리를 반영할 수 없다는 제한이 있다. 3GPP는 2008년 2월에 EPS-AKA (EPS-Authentication and key agreement)를 발표하였다〔12〕. 얼마 후, Sankaran C.B.는 EPS 구조와 EPS 구조상에서의 네트워크 접속 보안에 관한 튜토리얼을 소개하였다〔11〕.

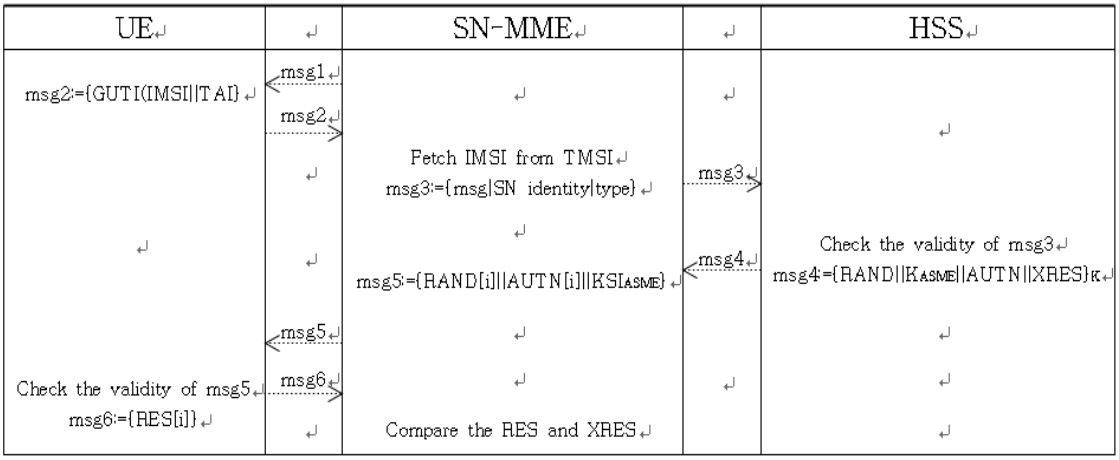
III. EPS와 EPS-AKA

이 장에서는 3GPP LTE/SAE in Release 8에서의 EPS의 인증과 키 동의 절차에 대해서 설명한다.

3.1 3GPP LTE/SAE 구조

3GPP LTE와 SAE는 OFDM기술과 평형 IP기반 구조로 빠른 데이터 속도를 제공하는 것을 목표로 하고 있다. EPS 구조는 3GPP LTE/SAE의 목표를 달성하기 위해 제안 되었다.

〔그림 1〕은 중요한 인터페이스들을 통해 EPS 구조를 보여준다. EPS는 접속 망(access network)과 코어 망(core network)으로 구성된다. 접속 망은 E-UTRAN(Evolved Universal Terrestrial



〔그림 2〕 NAS와 AS평면에서의 EPS인증과 키 동의

Radio Access Network)라고 불리고, 코어 망은 EPC(Evolved Packet Core)라고 불린다. EPS는 다중 접속 망(E-UTRAN, UTRAN, 그리고 GERAN을 포함한 3GPP 접속 망과 CDMA-2000, WiMAX, 그리고 WiFi를 포함하는 비 3GPP접속 망) 사이에서 작동할 수 있도록 정의 되었다〔13〕. 모든 무선 접속 프로토콜은 eNodeB라고 불리는 하나의 노드에서 관리되어져야 한다. 신호 조절 평면과 사용자 데이터 평면은 S1-MME와 S1-U 인터페이스를 통해 각각 E-UTRAN과 EPC사이에 설립된다. 모든 3GPP 종류의 접속 기술은 S-GW(Serving Gateway)를 통해 연결되고, 모든 비 3GPP 종류의 접속 기술은 일반적으로 P-GW(Packet data network GateWay)나 ePDG(evolved Packet Data Gateway)를 통해 연결 된다. MME(Mobility Management Entity)는 GERAN/UTRAN SGSN (Serving GPRS Support Node)과 같고 인증, 시그널링 보안과 이동성을 포함하는 조절 함수를 관리한다. 더 자세한 정보는 〔11〕〔13〕〔14〕에서 찾아 볼 수 있다.

3.2 EPS-AKA(Extended Authentication and Key Agreement)

All-IP EPC 네트워크의 취약성과 다양한 접속 기술의 상호작용 결핍을 없애기 위해, UMTS-AKA를 고친 EPS-AKA라고 불리는 새로운 인증과 키 동의(AKA)가 제안되었다. EPS-AKA에 대한 설명은 〔그림 2〕에 나타나 있다.

사용자 단말(UE)은 IMSI(International Mobile Subscriber Identity)라고 불리는 영구 신원을 msg1에 대한 응답을 통해 평문의 형태로 전송한다. 만약 사용자 단말이 이전의 MME가 EPS-AKA 절차 이후에 전송한 GUTI(Globally Unique Temporary Identity)를 이미 가지고 있었다면 TAI(Tracking Area Identity)와 함께 GUTI을 전송할 수도 있다. MME는 HSS에게 MEE의 모바일 네트워크 코드와 네트워크 타입(e.g. E-UTRAN)을 포함한 SN의 신원(serving network identity)과 함께 두 번째 메시지(msg2)를 전달한다. 만약 IMSI가 정당하다면 HSS는 K개의 인증 벡터 행렬(EPS-AVs)을 생성하여 msg4를 통해 MME에게 전송한다. 인증 벡터는 메시지 인증 코드(AUTN)와 파생키(K_{ASME})를 포함하여 HSS가 고른 난수(RAND), 사용자 단말로부터 6번째 메시지로 전송 받길 기대하는 기대값(XRES), 인증 토큰으로 구성된다. K_{ASME}는 CK, IK 그리고 SN의 신원을 이용한 해쉬 함수로부터 파생된다. MME는 K개의 인증 벡터 중에 하나를 선택하여 RAND〔i〕와 AUTN〔i〕를 사용자 단말에게 msg5를 통해 전송한다. 추가로 MME는 K_{ASME}의 인덱스인 KSI_{ASME}를 포함시킨다. 사용자 단말은 AUTN에 있는 메시지 인증 코드를 통해 MME를 인증하고 CK, IK 그리고 K_{ASME}를 생성한다. 또한 사용자 단말은 전송받은 KSI_{ASME}와 GUTI와 함께 K_{ASME}를 저장한다. msg6을 받으면 MME는 전송받은 RES〔i〕와 XRE〔i〕를 비교한다. 만약 둘이 일치하면 MME는 사용자 단말이 정당하다고 판단하고, 인증은 성공한다. EPS-AKA이후에

〔표 1〕 UMTS-AKA와 EPS-AKA의 보안 기능성 비교

기준	UMTS-AKA	EPS-AKA
취약성	redirection, 가짜 BS 공격에 취약	네트워크 identity를 포함함으로써 예방
인증	벡터 기반 AKA	벡터 또는 키 재사용 기반 AKA
ID 보호	TMSI, 제한적	GUTI, 제한적
키 요소	VLR이 인식하는 CK, IK	MME는 오직 K_{ASME}만 보유, CK와 IK는 없음
기밀성	AS 단계에서만 암호화	AS(시그널링과 데이터 모두)와 NAS(시그널링만)에서 암호화
무결성	AS단계에서만 무결성 보호	AS와 NAS단계에서 무결성 보호
핸드오버 지원	(1) SGSN 핸드오버, (2) GSM으로의 로밍	(1) X1, (2) S1핸드오버, (3) Inter RAT, (4) 비 3GPP와 상호작용

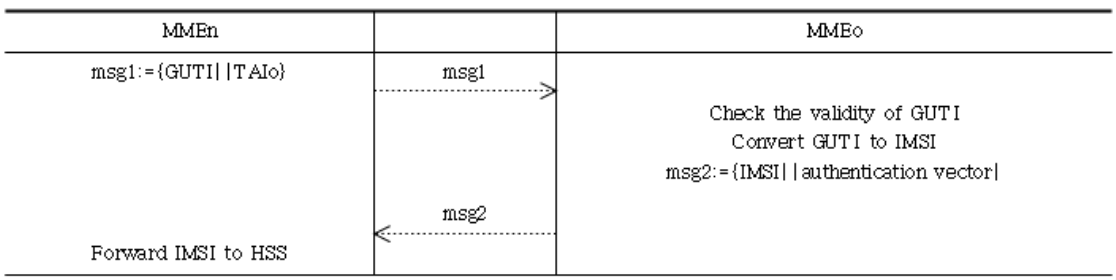
SMC(Security Mode Command)를 협상하기 위해 암호화와 완전성 알고리즘과 보안을 위해 작동 가능한 것들이 교환된다. EPS에는 두 가지의 SMC절차가 정의되있다: 하나는 사용자 단말과 MME간의 NAS(Non-Access Stratum)단계에서의 절차와 사용자 단말과 eNodeB간의 AS(Access stratum)단계에서의 절차가 있다.

3.3 EPS-AKA와 UMTS-AKA 비교

UMTS-AKA와 EPS-AKA사이의 차이는 〔표 1〕에 요약되어 있다. 가짜 BS(Base Station) 공격은 사용자 단말과 MME사이의 상호 인증을 강화해서 피할 수 있다. 사용자 단말은 SN의 신원을 통해 MME를 확인할 수 있다. 더욱 정교해진 키 구조로 인해 EPS-AKA를 수행할 필요성이 줄어서 MME는 한번에 오직 한 개의 인증 벡터를 가져 온다. 특히 서비스 요청은 EPS-AKA 절차 전체를 수행하지 않고, 저장된 K_{ASME}를 이용해서 인증 될 수 있다. 더욱이 인증 벡터의 묶음을 상호배치 하는데서 발생하는 재동기화 문제를 해결할 수 있다. 앞으로 3.2장에서 설명한 인증 방법을 인증 벡터 기반(authentication vector-based) EPS-AKA라고 부르고, 다른 방법을 저장된 K_{ASME} 키 재사용 기반(key reuse-based) EPS-AKA라고 하겠다. 더욱이 NAS 신호는 암호화되고, 이것의 완전성은 NAS와 AS 두 곳에서 확인된다.

eNodeB의 적용범위가 작아지고, 네트워크 접속 기술이 더 많아져서 핸드오버는 전보다 더 빈번하게 발생한다. EPS-AKA에서 제공하는 핸드오버 방법에는 4가지가 있다.

- X2 핸드오버: eNodeB 사이에 직접적으로 핸드오버가 발생할 수 있다. eNodeB는 X2 인터페이스를 통해 핸드오버 체인을 구성할 수 있다(〔그림 1〕 참조). 이전의 eNodeB는 K_{eNB}를 포함한 키 구성성분들을 현재의 eNodeB로 전송한다. 후방향 안정성(backward secrecy)를 보장하기 위해, K_{eNB}는 일방향 해쉬 함수로 새롭게 생성된 K_{eNB}^{*}로 바뀐다. 또한 MME는 전방향 안정성(forward secrecy)도 지원한다.
- S1 핸드오버: 하나의 서빙 네트워크 도메인에서의 IMSI와 보안 문맥(security context)의 배포는 EPS-AKA에 정의 되어있다〔1〕〔12〕. 관련 절차는 〔그림 3〕에 나타나 있다. 사용자 단말은 이전에 방문한 MMEo의 관할권 아래서 GUITo와 TAIo를 통해 확인된다는 점에서 S1 핸드오버 절차는 새 MMEn에 의해 호출된다. MMEo는 사용자 데이터를 찾고 추가적으로 사



〔그림 3〕 SN 도메인에서 IMSI와 보안 문맥의 분배

용되지 않은 EPS 인증 벡터나 현재의 보안 문맥을 포함하여 IMSI를 MMEn에게 전송한다.

- Inetr RAT: 사용자 단말은 UMTS의 SGSN과 EPS의 MME에 동시에 등록될 수 있다. MME는 K_{ASME}를 새로운 CK′와 IK′로 바꾸고 이것들을 문맥 응답 메시지(context response message)에 담아서 SGSN에게 전송한다. 대상이 된 SGSN은 저장된 CK와 IK를 전송받은 CK′와 IK′로 대체한다.
- 비 3GPP 네트워크와의 상호작용: 3GPP EPS와 비 3GPP 네트워크 사이의 이동성에는 세 가지 옵션이 있다: 프록시 모바일 IP, 모바일 IPv4 그리고 듀얼 스택 모바일 IPv6. 비 3GPP 네트워크가 무선랜의 경우처럼 신뢰받지 못한 네트워크일 경우 IPsec 터널(ePDG의 경우)이 구축된다.

IV. 분석 모델

이 장에서는 EPS-AKA에서 발생하는 시그널링 부하에 대해 모델링하고 평가하는 방법으로 갱신 과정과 갱신 보상 이론에 대해 소개한다.

4.1 시스템 모델과 분석

포아송 과정은 사건이 독립적이고 동일한 분포(i.i.d)를 갖는 지수적인 랜덤변수 일 때, 특정 시간 안에서의 계산과정 이다. 정규화 하는 하나의 방법은, 계산과정에서 특정시간 안의 사건이 임의의 분포로 i.i.d 일 때를 고려하는 것이다. 이러한 계산 과정을 갱신 과정〔9〕 이라고 한다. 음수가 아닌 랜덤 변수의 수열 $\{X_1, X_2, \ldots\}$에서 X_n이 계산과정에서 n-1번째와 n번째 사건 사이의 시간이라고 할 때, 계산과정 $\{N(t), t\geq 0\}$을 갱신 과정이라고 한다. 모든 갱신 사건 $\{S_n, n\geq 0\}$에서 갱신 과정은 완벽하게 재귀적이다. 갱신 간격이 $\{X_n, n\geq 0\}$인 갱신 과정에서 식(1)이 성립한다:

$$S_n = \sum_{i=1}^{n} X_i = S_{n-1} + X_n,\ where\ S_0 = 0 \qquad (1)$$

보상은 갱신 사건이나 갱신 주기 시간에 얻어진 것이라 가정하자. 보상은 갱신에 덧붙여진 비용이나 이익이다. R_n이 평균이 E〔R〕이고, n번째 갱신 X_n시간에서 얻어진 보상이라고 하자. R_n은 X_n에 의존성 있는 i.i.d 이다. 그러면 t시간동안 얻어진 총 보상 R(t)는 식(2)와 같다. 새로운 과정 {R(t), t≥0}를 갱신 보상 과정이라고 한다.

$$R(t) = \sum_{n=1}^{N(t)} R_n,\ where\ N(t) = \max\{n : S \leq t\} \qquad (2)$$

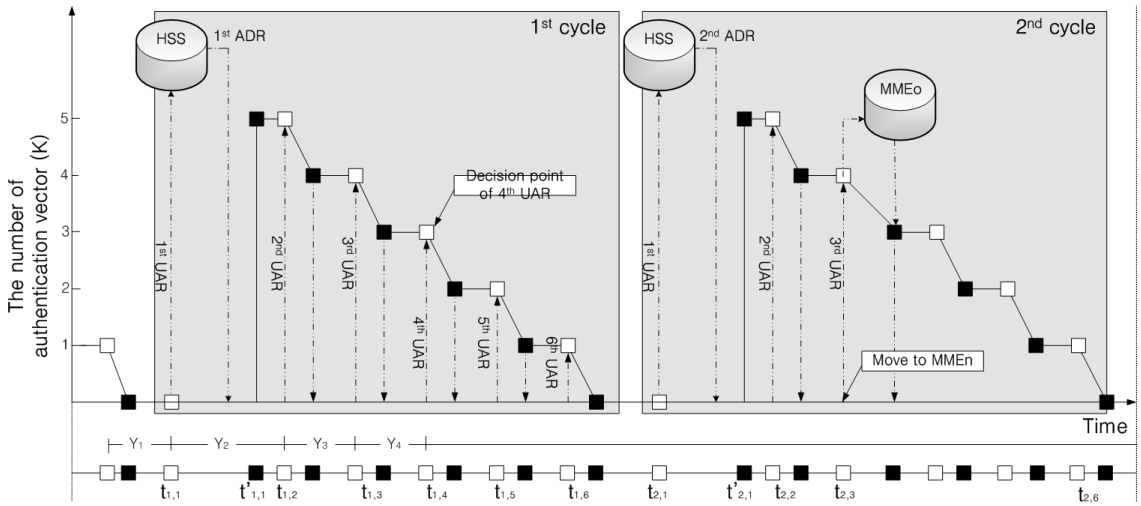
E〔R〕〈∞, E〔X〕〈∞ 일 때 {R(t), t≥0}이 갱신 보상 프로세스라고 하자. 그러면 긴 시간 동안의 보상율은 식(3)과 같다. 식(3)은 대수의 강한 법칙에 의해 증명된다.

$$\lim_{t\to\infty}\frac{R(t)}{t} = \lim_{t\to\infty}\frac{\sum_{n=1}^{N(t)} R_n}{N(t)}\frac{N(t)}{t} = \frac{E[R]}{E[X]} \qquad (3)$$

4.2 벡터 기반 방법에서의 시그널링 비용

EPS-AKA 절차는 아래의 이유로 인해 갱신 과정으로 해석할 수 있다. 갱신 사건은 HSS(벡터 기반 EPS-AKA)로 부터 가져온 모든 인증 벡터를 다 사용하거나 키 재사용 타이머가 만료되는 것을 말한다(키 재사용 기반 EPS-AKA). 더욱이 갱신 시도 시간은 다수의 인증 계기들(예. 통화/종료, X2 핸드오버, S1 핸드오버, 멀티미디어 요청, 등)의 매쉬업(mash-up)으로 인해 지수적인 분포를 따르지 않을 수 있다. 갱신 과정은 포아송 도착 과정에 제한되지 않고 임의의 랜덤 과정에도 사용될 수 있다. 게다가 갱신 보상 이론은 전체적인 비용을 긴 기간 동안 관찰하지 않고 계산할 수 있다. 결론적으로 우리는 EPS-AKA의 인증 시그널링 부하를 갱신 보상 이론을 적용하여 분석하였다. 본 논문에서 사용된 표기들은 〔표 2〕에 나열하였다.

〔그림 4〕는 벡터기반 EPS-AKA의 타이밍 다이어그램을 갱신 과정의 형태로 나타냈다. 인증 벡터의 수는 6개라고 가정한다. $t_{x,y}$와 Y_i는 각각 x번째 ADR에서 y번째 사용자 인증 요청(UAR)이 일어났을 때와 각 인증 이벤트의 기간을 나타낸다. $t_{1,1}$에서 사용자 단말은 처음으로 UAR 메시지를 사용한다. 그리고 HSS로부터 인증 벡터를 가져오고, 인증 데이터 요청/응답(ADR)을 통해 $t'_{1,1}$에서 종료한다. 채워진 것과 비어있는 사각형은 각각 UAR 이벤트에서 시작과 끝 지점을 나타낸다. $t'_{1,1}$에서 5개의 인증벡터가 유효하다. $t'_{2,3}$에서 S1 핸드오버가 발생했다고 가정하면, 3장에서 설명한 MME간에(MMEo와 MMEn) 문맥 전송이 발생한다. n번째 UAR이 시작할 때 (n+1)번째 UAR을 선택하기 위해 5개의 면을 가진 주사위가 매번 굴려진다고 하자. 예를 들면, 4번째 UAR은 세



〔그림 4〕 갱신 과정 형태의 인증 이벤트 타이밍 다이어그램

번째 UAR의 시작점인 $t_{1,3}$에서 선택된다. 갱신 간격의 기대 값은 Y_i와, HSS의 계산 지연과 HSS까지의 SIP 신호 비용의 전송 지연인 D의 조합으로 결정된다. Y_i는 각 인증 계기 X_i에 대해 p_i로 베르누이 분포를 따르기 때문에 식(4)에서 나타낸 것과 같이 확률 밀도 함수 $f(Y)$를 갖는다.

$$f(Y)=\sum_{i=1}^{M}P_i \cdot f(X_i), where \sum_{i=1}^{M}P_i=1 \quad (4)$$

갱신 보상 이론에 따르면 단위 시간당 비용은 보상의 기대 값인 E〔R〕을 갱신 간격의 기대 값인 E〔N〕으로 나눈 값으로 계산된다. 첫 번째로 갱신 간격은 식(5)에서 보이는 바와 같이 E〔D〕와, E〔Y〕를 (k-1)로 곱한 값으로 구해진다.

$$E[N]=(K-1)\cdot E[Y]+E[D] \quad (5)$$

두 번째로 갱신 비용의 기대 값은 C_i가 i번째 인증 계기 X_i를 완료 했을 때의 총 신호비용 이라고 할때 식(6)에 나타난 바와 같이 계산된다.

$$\begin{aligned} E[R] &= C_0+(K-1)\cdot E[Y]\cdot C_{i(1\le i\le M)} \\ &= C_0+\sum_{j=1}^{K-1} j\cdot(\sum_{i=1}^{M} p_i E[X_i]C_i) \end{aligned} \quad (6)$$

따라서 평균 비용 함수 C(K)는 식(7)과 같다.

$$\begin{aligned} C(K) &= \frac{E[R]}{E[N]} \\ &= \frac{C_0+\sum_{j=1}^{K-1} j\cdot(\sum_{i=1}^{M} p_i E[X_i]C_i)}{(K-1)\cdot E[Y]+E[D]} \end{aligned} \quad (7)$$

그렇지만 예외적인 이벤트 C_ϵ와 확률 P_ϵ을 고려해야 한다. 예외적인 인증 계기는 사용자 단말이 전원 꺼지거나, 다른 SN으로 S1 핸드오버를 하거나, 비 3GPP 접속기술로 로밍을 해서 갱신 과정을 떠날 때이다. 그 비용은 예외적인 상황이 발생할 때 까지 경계가 주어지므로 기하학적 랜덤 변수 $p_{\epsilon,k}=p_\epsilon\cdot(1-p_\epsilon)^k$에 영향을 받는다. 임의의 시도 시간에 따른 총 인증 시그널링 비용은 식(8)로 나타내진다.

$$C(K)=\frac{C_0+\sum_{k=1}^{k-1} p_{\epsilon,k}\cdot(\sum_{i=1}^{M}(K-1)p_i E[X_i]C_i)\cdot C_\epsilon}{(K-1)\cdot E[Y]+E[D]} \quad (8)$$

〔표 2〕 표기와 설명

표기	설명
K	가져온 EPS 인증 벡터의 수
T	K_{ASME} 재사용 만료 주기
M	인증 계기의 수 (M=5; 발신 EH는 멀티미디어 요청, X2 핸드오버, S1 핸드오버, Inter RAT)
p_i	i번째 인증 계기의 발생 확률 $(1\le i\le M)$
X_i	인증 계기의 도착 시간 간격
$F(x_i)$	$\Pr[X_i\le x_i], f(x_i)=(d/dx)F(x_i)$
$T(x_i)$	$\Pr[T\le x_i], t(x_i)=(d/dx)T(x_i)$
Y	X_i의 순열
C_i	i번째 인증 계기를 완료하는데 걸린 총 시그널링 비용
D	인증 벡터를 생성하는데 걸리는 SIP 시그널링 부하와 처리시간

4.3 키 재사용 기법에서의 신호 비용

CK와 IK는 MME에게 전송되지 않기 때문에 현재의 K_{ASME}를 사용한 재인증이 가능하다. 재인증을 하는 경우, 새로운 EPS-AKA 절차를 수행하지 않고 같은 K_{ASME}를 사용하여 오직 SMC만이 수행된다. KSI_{ASME}의 목적은 차후의 연결을 할 때 K_{ASME}를 재사용 가능하게 하기 위함이다. K_{ASME}가 손상되었거나 키 재사용 기간이 만료 되었을 경우 사용자 단말이 새로운 EPS-AKA 절차를 수행하는 정책을 가지고 있다고 가정하자. K_{ASME}가 손상되거나 만료되지 않으면, 대수의 강한 법칙에 따라 갱신 과정이 수행되어야 한다. 갱신 사건은 사용자 단말이 키 재사용 기반의 EPS-AKA 절차를 재시작 하여서 이전의 K_{ASME}를 새로운 것으로 바꾸는 경우를 말한다. Y_i가 EPS-AKA를 i번째 재시작 하는 순간이라고 할 때, 재사용 주기의 기대값 E[N]은 식(9)와 같다. $T(x_i)$는 K_{ASME}의 지속시간에 대한 누적 밀도 함수이다.

$$\begin{aligned} E[N] &= \int_0^{\infty} E(Y|X_i = x_i)dT(x_i) \\ &= \int_0^{T} x_i \cdot t(x_i)dx_i + \int_T^{\infty} T \cdot t(x_i)dx_i \\ &= \int_0^{T} [1 - T(x_i)]dx_i \end{aligned} \quad (9)$$

K_{ASME}이 손상되어서 EPS 네트워크의 모든 개체들이 키를 재생성 해야 하는 경우의 추가 비용을 C_{-1}이라고 하자.

$$\begin{aligned} E[R] &= (C_{-1} + C_i) \cdot \\ &\quad \int_0^{T} t(x_i)dx + C_i \cdot \int_T^{\infty} t(x_i)dx \\ &= (C_{-1} + C_i) \cdot T(T) + C_i \cdot [1 - T(T)] \end{aligned} \quad (10)$$

식(9)와 식(10)에 기초하여, 임의의 시도시간에서 총 인증 시그널링 비용은 식(11)과 같다. 벡터 기반의 방법에서는 자명할지라도 간소함을 위해 이 식에서 확률 p_ϵ에 의한 예외적 이벤트는 고려하지 않았다.

$$C(T) = \sum_{i=1}^{M} p_i \cdot \frac{(C_{-1} + C_i) \cdot T(T) + C_i \cdot [1 - T(T)]}{\int_0^{T} [1 - T(x_i)]dx_i} \quad (11)$$

4.4 각 인증 계기에 따른 비용함수

각 인증 계기에 따른 비용함수 $C_i (0 \le i \le M)$를 명확히 정량화 할 필요가 있다. 각각의 인증 사건에 대해 EPS 개체들과 서비스 절차들 사이의 메시지 교환은 [13]에 나타나 있다. [표 3]에서 인증 계기와 그와 관련된 메시지 교환은 C_{A-B}(EPS 개체 A가 B와 통신)의 형태로 표현되어 있다. 여기서 게이트웨이, 정책 서버와의 통신인 업링크와 다운링크 데이터는 배제하였다. 일반적으로 LTE 표준에서 RRC 신호 지연과 사용자 제어 평면 지연은 각각 10ms와 100ms만큼 지연된다. 또한 사용자 단말과 eNodeB 사이의 3가지 케이스의 메시지 교환을 정규화 하였다: 코어 망 내부, 네트워크를 가로지르는 것을 각각 $\alpha, \beta, \text{and} \delta$로 표현. 홉의 수가 늘어감에 따라 코어 망 안에서의 RTT가 무선 접속 네트워크 안에서의 RTT보다 더 느려지는 경향을 보였다. 따라서 정규화된 점근적인 신호 비용들 사이의 관계는 $\delta \ge \beta \gg \alpha$로 표현된다.

C_1은 네트워크에서 시작되었는지(통화 종료) 사용자 단말에서 시작되었는지(통화 연결)에 의존한다. 수신전화의 경우에 페이징 관련 신호들만이 교환되는 것에 비해 발신전화의 경우 추가적인 라디오 베어러(radio bearer) 생성과 베어러 갱신 비용이 많이 발생한다. 멀티미디어 요청은 제 3자와 연관된다. 멀티미디어 브로드캐스트 멀티캐스트 서비스(MBMS)는 이러한 인증 계기로 사용 할 수 있다. 핸드오버($C_3, C_4 \text{and} C_5$)에 따라 관측지역 갱신 과정 (C_{TAU})는 S-GW 재배치 과정 없이 수행 되어야 한다.

V. 수치적인 결과

인증 신호 부하를 분석하기 위해 갱신 과정을 적용하여 포아송 가정을 완화 하였다. 그리고 인증 계기를 다섯 가지 서비스 요청으로 구분 하였다(예. 통화, 멀티미디어, X2, S1 그리고 UMTS 핸드오버). 이번 장에서는 제안한 분석 모델을 통해 인증 트래픽 부하를 평가하는 예를 보일 것이다.

5.1 지수함수를 이용한 기준선 비용 함수의 분석

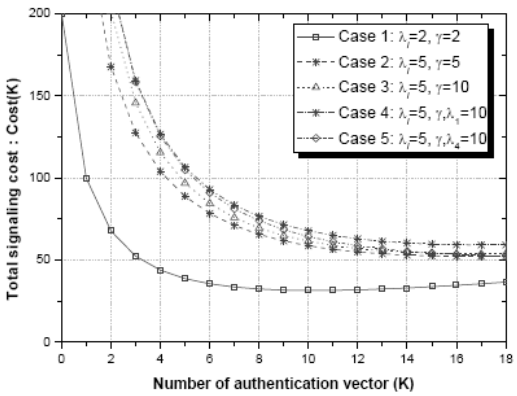
모든 인증 계기에 대해 지수분포를 이용한 기준선 비용 함수 C(K)를 분석한다. i번째 인증 계기는 통화 처리 속도 λ_i에 대해 지수 분포를 따른다고 가정한다. i번째 사건이 발생할 확률은 균일하게 분포 한다. 이러한 가정에 기반 하여, 인증 벡터를 가져오는 지연시간이 속도 Υ에 대해 지수 분포를 따른다고 할 때 갱신 간격의 기대 값은 식(8)과 같다.

〔그림 5〕는 모든 인증 계기에 대해 총 시그널링 비용 함수 C(K)의 지수분포를 나타낸다. 총 시그널링 비용 함수는 K가 증가함에 따라 볼록한 형태를 가진다. 최적화된 K′값은 C(K)를 최소화 하는 값이다. 시도 속도가 $\lambda_i = 2$ (Case 1)에서 $\lambda_i = 5$ (Case 2)로 증가하면, 총 시그널링 비용은 10.21과 16.71사이의 값인 K′에서 최소 값을 가질 것이다. Case2와 Case3에서 보이는 바와 같이 셋업 배포 속도(setup distribution rate) γ값을 증가시키는 것의 영향은 그다지 크지 않다. 가장 큰 시그널링 비용(4번째 인증 계기)일 때 시도 속도의 증가는 시그널링 비용의 뚜렷한 증가를 보였다.

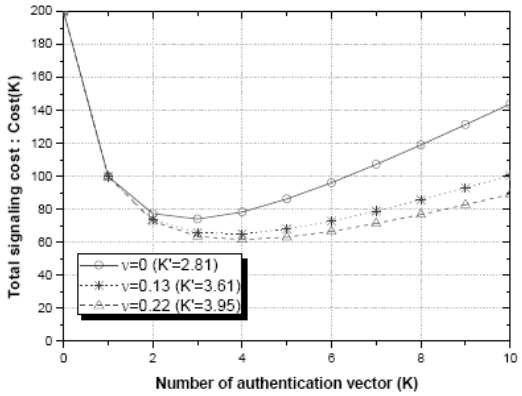
〔그림 6〕은 같은 평균 속도를 갖는 분포 패턴 p_i의 민감성을 보여준다. 분산에 따른 3가지 그룹을 비교하였다. 분산이 낮으면, 비용 함수 C(K)는 증가하는 반면에 최적화 K는 감소한다. 이러한 현상의 이론적 근거는 아래와 같다: 만약 가입자가 특정 이벤트(e.g. 10대 아이들 사이에 인기 있는 멀티미디어 서비스)에 기우는 경향이 있으면, 놀랍게도 그 가입자는 여러 이벤트를 사용하는 가입자에 비해 전체 EPS 시스템을 흔들지 않는다.

p_ϵ는 갱신 과정에서 벗어나는 확률이다. 〔그림 7〕은 예외적인 경우의 영향을 보여준다. p_ϵ값이 크면, 총 시그널링 비용은 명백히 증가하고 K값은 시스템 자원의 낭비를 줄이기 위해 감소해야 한다. 사용자 단말이 10퍼센트의 확률로 습관적으로 전원이 꺼지거나 다른 접속 기술로 로밍해 간다면 벡터 기반의 EPS-AKA는 의미 없게 된다(K′〈1).

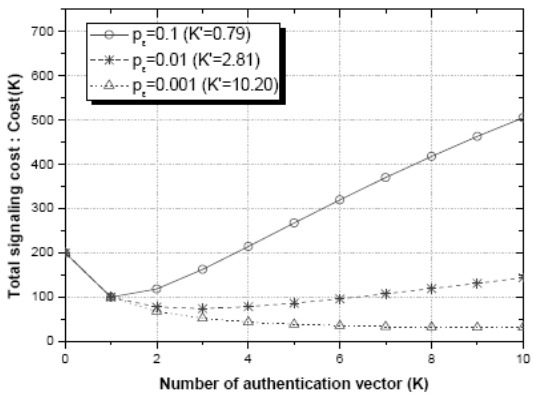
〔그림 8〕은 비용 함수 비율에 따른 3개의 다른 시도 속도의 배열을 나타낸다. 비용 함수는 $C_1 < C_2 < C_3 < C_5 < C_4$와 같은 관계를 갖는다. 인증 이벤트의 발생 속도의 지수 분포가 평균값을 유지하면서 정비례와



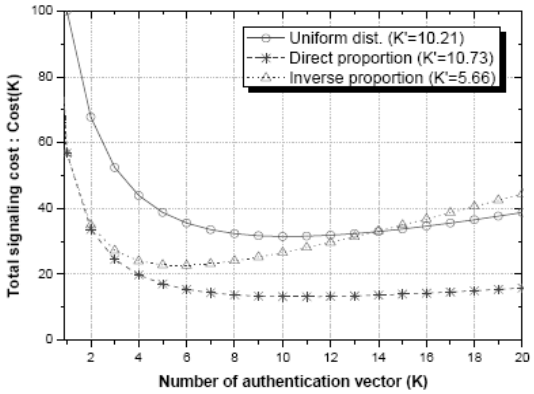
〔그림 5〕 지수적 시도 속도에 따른 총 시그널링 비용



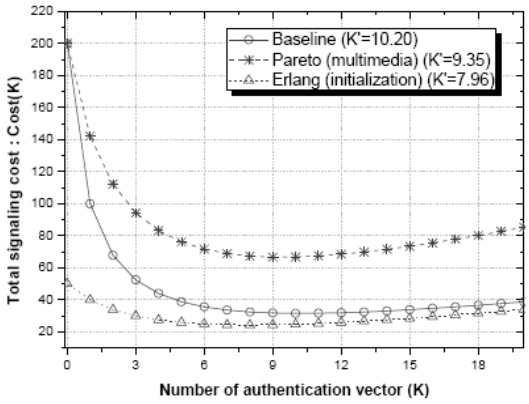
〔그림 6〕 발생확률에 대한 분산의 영향$(\lambda_i = 1)$



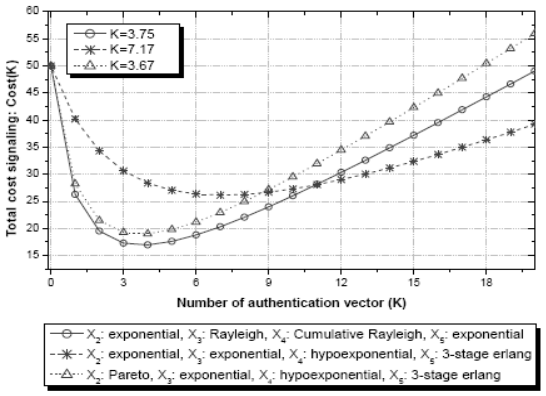
〔그림 7〕 예외조건에 대한 민감성$(\lambda_i = 1)$



〔그림 8〕 시도 속도에 따른 비용 함수 비율의 영향
$(p_i = 0.2, p_\epsilon = 0.001)$



〔그림 9〕 파레토와 엘랑 분포의 영향



〔그림 10〕 핸드오버에 대한 다양한 연속 랜덤 프로세스의 조합

반비례 관계를 따른다고 가정한다.

5.2 다양한 랜덤 과정의 영향

고정된 평균값을 갖는 일반적인 발생시간에 대한 다른 분포들에 대해 고려하였다: 지수분포, 초 지수분포, 엘랑(감마)분포, 레일리(Rayleigh) 분포. 통화 발생에 대해 전통적인 지수분포는 적절하지 않다. 포아송 과정이 연관되어 있지 않다고 하더라도 지수분포, 초 지수분포 또는 엘랑분포를 통화 발생에 대해 적용하는 것은 큰 차이를 보이지 않는다〔6〕. 대신에 〔15〕의 저자는 telnet, smtp, ftp연결 등의 다양한 인터넷 기반의 어플리케이션의 특성에 대해 표현하기 위해 많은 수의 분석적인 랜덤 변수를 사용하였다. 그에 따르면 파레토 분포(Pareto distribution)가 멀티미디어 요청에 대한 시뮬레이션에 적합하다. 또한 log2-normal과 log2-extreme 분포는 자기 유사성과 heavy-tail 특성을 갖기 때문에 통화 발생 요청에 적합하다.

파레토 분포는 웹 트래픽을 정확하게 근사치를 구하는데 널리 사용되곤 한다. i=2(멀티미디어 요청의 경우)일 때 파레토 분포에서 매개변수 α와 β는 각각 1.2와 $(\alpha-1)/\alpha \bullet \lambda_i$로 설정 된다. 더 나아가 초기 인증 벡터를 가져오는 단계에서 엘랑 분포를 사용하였다. 〔그림 9〕에 있는 결과는 과소평가 받는 파레토를 제외한 기준선 분포를 보여준다. 파레토 분포에서 멀티미디어 요청에서 필요한 인증의 수는 감소하였지만 전체적인 인증 시그널링은 증가하였다.

〔그림 10〕에서는 오직 핸드오버 프로세스 (X_3, X_4, X_5)와 멀티미디어 요청(X_2)에만 적용할 수 있는 변수들의 다양한 조합을 조사하였다. 2차원 벡터가 서로 연관이 없으며 같은 분산을 갖는 정규분포일 때 레일리 랜덤 변수는 발생할 수 있다. 이러한 레일리 과정의 특성들은 가입자의 속도와 eNodeB에 의한 셀 적용범위로 구성된 핸드오버를 설명할 수 있다. 다양한 사용자 패턴에 대한 모델링을 〔그림 10〕을 통해 알 수 있다. 어떤 특정한 조합이 다른 조합보다 좋다고 할 수는 없다. 하지만 주어진 인증 이벤트 분포에 관한 다양한 조합을 통해 우리는 인증 벡터의 수의 최적화 값을 찾을 수 있다.

VI. 결 론

통합된 4G 서비스는 다양한 핸드오버와 인증 시그널링 비용을 지원하도록 요구한다. 본 논문은 인증에 관한 절차와 EPS 네트워크에서 사용된 핸드오버의 종류에 대해서 소개 하였다. 인증 신호 부하에 대해 분석하고 평가할 수 있는 정교한 수학적 틀을 제안하였다. 또한 다양한 성능 매개변수의 영향에 대해 조사하였다. 그 결과를 보면 작은 분산에서 최소 비용 함수가 점차 줄어들 때 최적화 K값은 감소한다. 멀티미디어 요청에서 파레토 분포는 인증 요청의 수는 감소하는 반면 전체적인 인증 시그널링은 증가한다. 그리고 적절한 eNodeB 핸드오버에 필요한 레일리 분포에 대해 조사하였다. 우리는 이동성 관리, 보안정책, 그리고 다양한 랜덤 발생 프로세스에 대한 필요성을 확립하였다. 제안된 모델과 결과에 기반을 둔 시스템 매개변수의 평균을 구하는 것이 중요하다. 마지막으로 현실의 상황에 대한 적합성을 증가시키기 위해서는 차후 연구가 필요하다.

참고문헌

〔1〕 Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, "Security Architecture (Release 7)," 3GPP TS 33.102 version 7.1.0, Dec. 2006.

〔2〕 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), vol. 1, pp. 392-397, Mar. 2005.

〔3〕 Ja′afer Al-Saraireh and Sufian Yousef, "A new authentication protocol for UMTS mobile networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, no. 2, pp. 1-10, Apr. 2006.

〔4〕 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, pp. 493-501, May 2003.

〔5〕 Yan Zhang and Masayuki Fujise, "An improvement for authentication protocol in third-generation wireless networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2348-2352, Sep. 2006.

〔6〕 Yan Zhang, Shaoqiu Xizo, Mingtuo Zhou and Masayuki Fujise, "Authentication traffics modeling and analysis in next generation wireless networks," *Wiley Wireless Communications and Mobile Computing*, vol. 8, no. 5, pp. 615-625, Jan. 2007.

〔7〕 Lin-Yi Wu and Yi-Bing Lin, "Authentication vector management for UMTS," *IEEE Transactions on Wireless Communications*, vol. 6, no. 11, pp. 4101-4107, Nov. 2007.

〔8〕 Ja'afer Al-Saraireh and Sufian Yousef, "Analytical model for authentication transmission overhead between entities in mobile networks," *Elsevier Computer Communications*, vol. 30, no. 8, pp. 1713-1720, Jun. 2007.

〔9〕 Sheldon M. Ross, Introduction to probability models, 8th Ed., Academic Press, Dec. 2002.

〔10〕 Dario S. Tonesi, Luca Salgarelli, Yan Sun and Thomas F. La Porta, "Evaluation of signaling loads in 3GPP networks," *IEEE Wireless Communications*, vol. 15, no. 1, pp. 92-100, Feb. 2008.

〔11〕 Sankaran C. B., "Network access security in next-generation 3GPP systems: A Tutorial," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 84-91, Feb. 2009.

〔12〕 Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE), "Security Architecture Security (Release 8)," 3GPP TS 33.401 version 8.2.1, Dec. 2008.

〔13〕 Third Generation 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," 3GPP TS 23.401 version 8.4.1, Dec. 2008.

〔14〕 Third Generation Partnership Project; Technical Specification Group Radio Access Network. "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," 3GPP TS 36.300 version 8.7.0, Dec. 2008.

〔15〕 Vern Paxson, "Empirically derived analytic models of wide area TCP connections," *IEEE/ACM Transactions on Networking*, vol. 2, no. 4, pp. 316-336, Aug. 1994.

〈著者紹介〉

강 성 용 (Seong-Yong Kang) 학생회원
2011년 2월: 성균관대학교 컴퓨터공학과 학사졸업
2011년 3월~현재: 성균관대학교 휴대폰학과 석사과정
〈관심분야〉 3GPP 이동통신 보안

한 찬 규 (Chan-Kyu Han) 학생회원
2006년 8월: 성균관대학교 컴퓨터공학과 학사졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사졸업
2012년 2월: 성균관대학교 휴대폰학과 박사졸업
2012년 3월~현재: 삼성전자 근무
〈관심분야〉 3GPP 이동통신 보안

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 학사 졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사졸업
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사졸업
2001년~2004년: Lancope 근무
2004년 3월~현재: 성균관대학교 정보통신공학부 부교수
〈관심분야〉 네트워크보안, Traffic characterization and modeling