인증 시그널링 트래픽 최소화를 위한 수학적 분석에 관한 연구

한찬규*, 송세화**, 최형기**
*성균관대학교 휴대폰학과
**성균관대학교 정보통신공학부
e-mail : {hedwig, shsong, hkchoi}@hit.skku.edu

Analytical Model for Reducing Authentication Signaling Traffic in 3GPP Networks

Chan-Kyu Han*, Sehwa Song**, Hyoung-Kee Choi*
* Department of Mobile Systems Engineering, Sungkyunkwan University
** School of Information & Communication Engineering, Sungkyunkwan University

요 약

모바일 서비스는 사용자보호를 위해 인증 및 암호화 기능이 필수적으로 제공되어야만 한다. 3GPP 는 3 세대 이동통신 (UMTS)를 위한 인증보안구조인 AKA 를 정의하였다. AKA 에서는 인증벡터를 다수 개 생성하여 처리하는 기법을 채택하고 있으나 이러한 기법이 인증서버의 load 증가 및 방문서버의 저장공간 소모라는 문제점을 야기한다. 하지만 인증벡터를 다수 개 생성하는 기법은 단말의 핸드오버를 위한 필수불가결한 기법이다. 따라서 본 논문에서는 사용자의 이동패턴 및 인증요청 처리 속도에 따른 인증벡터의 동적 선택 알고리즘을 제안하여 이동통신 네트워크의 signaling load 를 최소화하고자 한다. 이를 위해 확률 및 큐잉 이론이 도입되었으며, 시뮬레이션을 통해 수학적 분석을 검증한다. 또한 기존 관련연구에서 제안 하는 알고리즘과 비교 평가하였다.

1. 서론

사용자의 이동성을 보장하며 음성 및 영상서비스를 지원하는 모바일 서비스가 대두되고 있다. 그러나 모바일 환경에서는 매체의 특성 때문에 공격자가 사용자의 통신정보, 개인정보를 도청할 수 있는 위협이 심각하다. 이를 막기 위해 암호화 기능을 제공하거나, 사용자 인증 기법을 제공하는 등 사용자의 안전과 비밀통신을 보장하는 보안이 반드시 제공되어야만 한다.

3rd Generation Partnership Project(3GPP)에서는 모바일 환경에서 사용자 인증 및 암호화, 메시지 인증키 생성을 제공하기 위해 Authentication and Key Agreement (AKA) 표준을 발표하였다 [1]. AKA 에서는 단말을 소유한 사용자, 방문자위치레지스터(Visitor Location Register:VLR), 홈위치레지스터(Home Location Register:HLR)가 관여하여 단말과 VLR 간의 상호인증 및 키 생성을 정의하고 있다. 하지만 AKA 의 특성상 VLR 과 HLR 즉 코어네트워크 내에서 signaling load 의 양이 3 세대 이동통신의 요구사항을 만족시키지 못 하고 있다. 이에 코어네트워크의 signaling load 를 줄이기 위한 연구가 다수 진행되었지만, 제안기법에 의존적이고 표준과의 호환성이 적다는 문제점이 있다.

HLR 에서는 단말의 인증 요청 시에 핸드오버를 고려하여 VLR 에게 다수의 인증벡터를 전달하는 매커니즘이 정의되어 있다. 하지만 상세한 단위가 정의되어 있지 않고, 네트워크 상황을 고려하고 있지 않은 정적(static) 선택 기법이다. 따라서 단말의 핸드오버 및 HLR/VLR 의 로드를 최소화 시키는 적절한 수의 인증벡터를 선택하여야 한다. 이에 본 논문에서는 TS 33.102 [1]에서 정의하고 있는 기존 인증시스템을 벗어나지 않고, 효율적으로 signaling load 를 관리할 수 있는 기법으로 동적(dynamic) 인증벡터 선택에 관한 연구를 진행하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 관련연구를 소개하며, 3 장에서는 3GPP AKA 의 기본 매커니즘을 소개한다. 4 장에서는 3GPP AKA 의 signaling load 에 관해 분석하고, 인증벡터 생성방식이 비효율적임을 지적한다. 5 장에서는 새로운 동적 인증벡터 선택 기법을 제안하고, 기존의 3GPP AKA 방식 및 관련연구와 비교한다. 6 장에서는 본 논문의 결론을 맺는다.

2. 관련연구

Chung-Ming Huang 들은 인증요청을 수신한 HLR 이 VLR 에게 단말의 인증정보를 전송할 때 발생하는 AKA 의 문제점에 대해 연구하였다[2]. Chung-Ming Huang 들은 인증정보를 다수 개를 전송하는 기법이 VLR 의 저장소와 HLR 과 VLR 간의 대역폭을 낭비한다는 문제점을 지적하였다[2]. Ja’afer Al-Saraireh 등[3]은 HLR 에의 signaling load 가 bottelneck 을 유발시킨다고 지적하였다. 그들은 AKA 의 구조를 역으로 바꾸어 reverse version of AKA 를 제시하였다. Reversed AKA 에

서는 HLR 대신에 단말이 인증벡터를 생성하며, 논문에서는 ns-2 시뮬레이션에 기반하여 signaling traffic 을 감소시킬 수 있다고 주장한다. 한편, Yi-Bing Lin 들은 같은 문제를 지적하고 3GPP AKA 를 수학적으로 분석하였다[4]. Ja'afer Al-Saraireh 등은 [4]의 저자들의 알고리즘을 비판하고, AKA 동적으로 결정하는 새로운 알고리즘을 정의하였다.

3. 3GPP AKA

본 장에서는 3GPP 의 대표적인 3 세대 이동통신 네트워크 구조인 UMTS 와 UMTS(3GPP)의 인증구조인 AKA 에 대해서 설명한다.

Third Generation Partnership Project(3GPP)에서는 1) 모바일 사용자와 네트워크 간 상호인증, 2) 메시지 인증키 및 암호화키 생성을 위해 Authentication and Key Agreement(AKA)를 정의하고 있다[1]. AKA 는 단말과 HLR 이 사전 공유한 비밀키 k 를 통해 VLR 과 단말 간의 상호인증을 수행하고 메시지 인증키 및 메시지 암호화 키를 생성하는 과정을 정의한다. 그림 1 에서 보듯이 AKA 는 MS 와 VLR 그리고 HLR 간에 6 단계의 메시지 교환으로 정의된다.

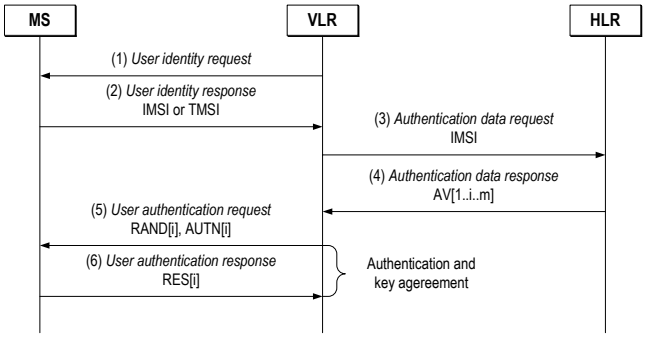

그림 1. 3GPP AKA 의 인증 구조

메시지 (1) ~ 메시지 (3)에서 보듯이 단말은 VLR 에게 자신의 IMSI 또는 TMSI 를 이용하여 인증을 요청하고, VLR 은 단말의 IMSI 를 통하여 HLR 에게 단말의 인증, 암호화 키 및 메시지인증 키 생성을 요청한다. 인증요청을 수신한 HLR 은 단말과 사전 공유한 비밀키 k 와 난수 *RAND* 를 선택하여 $\boldsymbol{m}$ 개의 *Authentication Vector(AV)*를생성하여 VLR 에게 전송한다. 각 AV 는 *RAND, XRES< CK, IK, AUTN* 으로 구성된다. *RAND* 는 HLR 이 생성한 난수이며, *CK* 는 암호화키, *IK* 는 메시지 인증키이며 *XRES* 는 정상적인 단말에 대해 VLR 이 기대하는 응답메시지이다. 각 요소는 다음과 같이 HLR 과 단말이 공유하는 함수 *f1,f2,f3,f4,f5* 에 비밀키 k 와 *RAND* 를 인자값으로 입력하여 생성한다. 메시지 (4)에서 HLR 로부터 m 개의 AV 를 수신한 VLR 은 그 중 i 번째의 AV 인 *AV(i)*를 선택함. *AV(i)*에 포함된 *RAND(i)*와 *AUTN(i)*을 단말에게 전송한다. 단말은 *RAND(i)*와 비밀키 k 를 통해 *AV(i)*를 구성하는 *CK(i), IK(i), XRES(i), AUTN(i)*를 생성하여 *AUTN(i)*의 *MAC(i)*을 검사한다. *MAC(i)*이 변조되지 않았다면, *SQN(i)*을 검사하여 *AV(i)*가 Replay 공격 등에 악용되지 않았는지를 검사한다. *AUTN(i)*의 *MAC(i)*에 대한 무결성과 *SQN(i)* 범위에 대해 확인하여 단말은 VLR 을 인증하고, 단말은 *RES(i)*를 계산하여 VLR 에게 보내고, VLR 은 HLR 으로부터 받은 *XRES(i)*와 단말이 보낸 *RES(i)*가 같은지 확인하고, 같다면 인증을 완료한다. 인증이 완료된 후에 VLR 과 단말은 *CK(i)*와 *IK(i)*를 이용하여 메시지 암호화 및 인증을 수행하고 비밀통신을 시작한다.

4. 3GPP AKA Signaling Load 분석

3 장에서 살펴봤듯이, 인증요청 시에 HLR 은 m 개의 인증벡터를 생성하여 VLR 에게 전송한다. 또한 VLR 은 핸드오버를 고려하여 단말의 인증벡터를 저장한다. 따라서 이는 (1) HLR 과 VLR 의 대역폭 소모, (2) VLR 저장공간 소모의 문제점이 있다. 하지만 다수개의 인증벡터를 생성/저장하는 것은 단말의 핸드오버를 고려하여 필수불가결하다. 예를 들어 [2]에서처럼 인증벡터의 개수를 단순히 1 개로 줄이면, 1 번의 인증 시 signaling load 는 줄어들지만 단말의 핸드오버가 잦다면 인증요청이 증가하므로 결국 signaling load 는 증가한다. 따라서 결론적으로 적절한 인증벡터의 개수 선택이 요구되며, [1]에서는 이를 제시하고 있지 않다. 본 논문에서는 3GPP AKA 의 signaling load 를 분석한 뒤 적절한 선택알고리즘을 제시하기로 한다.

단말이 VLR 의 영역으로 접근 후에 인증절차는 그림 2과 같다. 단말은 User Authentication Request/Response(UAR) 메시지를 통해 VLR 에게 인증을 시작한다. VLR 은 자신의 저장공간에 인증벡터가 없으면 HLR 로 Authentication Data Request/Response (ADR)을 전송한다. VLR 이 m 개의 인증벡터를 수신한 뒤에, 인증은 오직 MS 와 VLR 사이에 UAR 메시지를 통해서만 이루어진다.$t_{1,m}$ 에서 보면 인증벡터가 소모되었으므로 $t_{2,1}$ 에서 새로운 인증벡터를 요구한다. 마지막 ADR 에서 ($t_{m,1}$) 단말은 오직 i 개만을 소모하였고 이 때의 UAR 은 $(n\text{-}1)m+i$ 번, 그리고 ADR 은 N 번만큼 발생하였다.

단말의 인증요청, 즉 호/핸드오버가 비율이 λ인 Poisson process 를 따른다고 가정하고, $\Theta(n,m,\tau)$를 특정 구간 τ 에서 n 번의 ADR 이 발생할 확률이라고 가정하자. 이 때 n ADR 은 $(n\text{-}1)+k$ $(1<k<m)$인 상황에서 발생한다. Poisson 확률분포에 따르면 $\Theta(n,m,\tau)$은 다음의 식 1 과 같이 계산된다.

$$\theta(n,m,\tau)=\sum_{k=1}^{m}\left\{\frac{(\lambda\tau)^{(n-1)m+k}}{[(n-1)m+k]!}\right\}e^{-\lambda\tau} \quad (1)$$

단말이 VLR service area 에서 머무르는(residence) 시간을 t 라고 가정하고, t 는 pdf 가 $f(t)$를 따른다고 한다. 이 때 MS 가 해당 VLR 에서 머무르는 동안 n ADR 이 발생할 확률 $P(n,m)$은 식 2 와 같다.

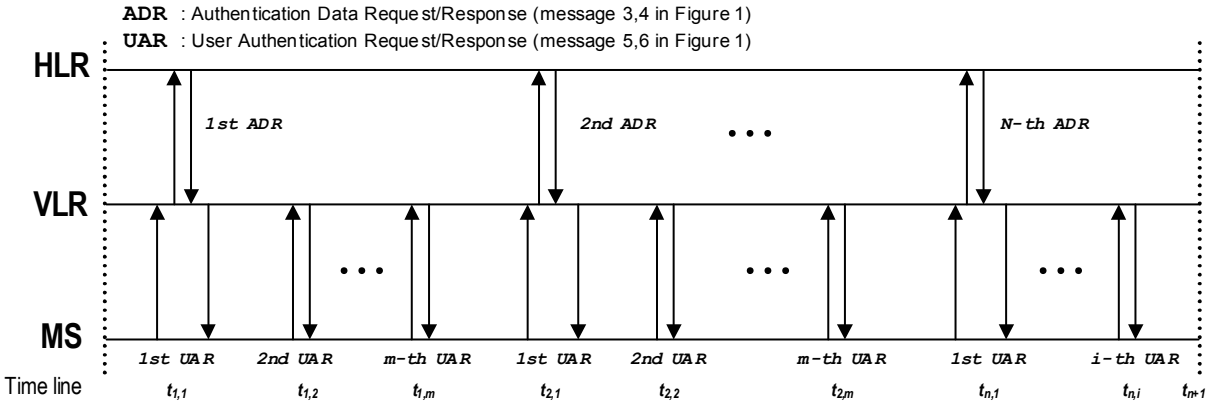

그림 2. 3GPP AKA 의 시간 도메인 그림

$$P(n,m)=\int_{t=0}^{\infty}\theta(n,m,t)f(t)dt \qquad (2)$$

위 식을 Laplace 변환($f^*(s)=\int_{t=0}^{\infty}f(t)e^{-st}dt$)을 통하여 정리하면 식 3 과 같다.

$$\begin{aligned}P(n,m)&=\sum_{k=1}^{m}\int_{t=0}^{\infty}\left\{\frac{(\lambda\tau)^{(n-1)m+k}}{[(n-1)m+k]!}\right\}e^{-\lambda\tau}f(t)dt\\&=\sum_{k=1}^{m}\left\{\frac{\lambda^{(n-1)m+k}}{[(n-1)m+k]!}\right\}\int_{t=0}^{\infty}t^{(n-1)m+k}\times e^{-\lambda\tau}f(t)dt \quad (3)\\&=\sum_{k=1}^{m}\left\{\frac{\lambda^{(n-1)m+k}}{[(n-1)m+k]!}\right\}(-1)^{(n-1)m+k}\times\left[\frac{d^{(n-1)m+k}f^*(s)}{ds^{(n-1)m+k}}\right]_{s=\lambda}\end{aligned}$$

E[N]은 ADR 의 기대 값이며, 식 4 와 같이 계산될 수 있다.

$$E[N]=\sum_{n=1}^{\infty}nP(n,m) \qquad (4)$$

이 때 VLR 에 머무르는 $f(t)$를 지수분포(exponential distribution)을 가정하고, 지수분포의 평균을 $1/\mu$라 하면, $P(n,m)$과 $E[N]$ 그리고 signaling load 인 $C(m)$은 각각 식 5, 6, 7 과 같이 계산될 수 있다.

$$P(n,m)=\left(\frac{\lambda}{\lambda+\mu}\right)^{(n-1)m}\left[1-\left(\frac{\lambda}{\lambda+\mu}\right)^{m}\right] \qquad (5)$$

$$E[N]=\frac{1}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^{m}} \qquad (6)$$

$$C(m)=E[N]\times(m+2\alpha)=\frac{m+2\alpha}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^{m}} \qquad (7)$$

위 식 7 의 a는 SS7 또는 SIP message overhead 를 나타낸 것이다.

그림 3은 ADR 전송에 따른 전체적인 signaling load 를 보여주고 있다. 각기 다른 λ 에 따른 signaling load 가 최소가 되는 지점이 적절한 m 값이 될 것이다.

결론적으로 인증벡터의 개수 m 은 (1) 단말이 해당 네트워크의 머무르는 시간 (μ), 과 (2) 단말의 인증요청 속도 (λ)에 따라서 동적으로 변화되어야만 한다.

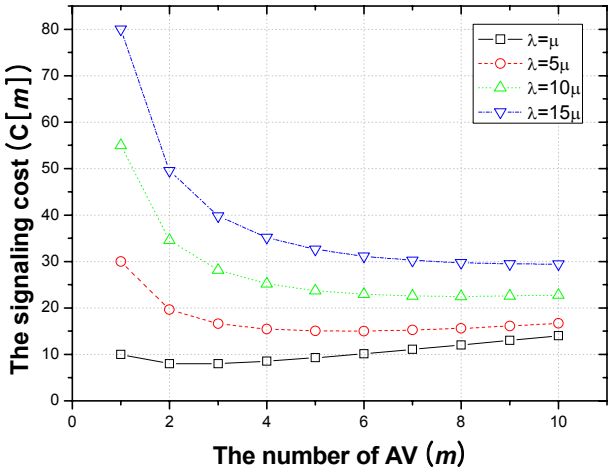

그림 3. ADR 전송에 따른 signaling load

5. 제안 알고리즘 및 비교

본 논문에서는 AKA signaling load 를 최소화하기 위한 동적 선택 알고리즘을 제시하고자 한다. 이 기법은 단말의 인증요청 속도와, 단말의 핸드오버 패턴에 따라서 변화한다. HLR 은 각 단말의 UAR/ADR 의 개수를 저장하는 역할을 수행하여야만 하며, 단말이 새로운 VLR 로 핸드오버할 시에 적절한 m 을 예측한다. 논문에서 제안하는 알고리즘은 다음의 식 8 와 같다.

$$m_t=(1-\alpha)m_{t-1}+\alpha\frac{Total\ number\ of\ UARs_{t-1}}{T_{i+1}-T_i} \qquad (8)$$

시뮬레이션은 random number generator 를 구현하여 perl 로 작성하였고, 지수분포 난수 생성은 inversion 기법을 사용하여 계산하였으며, 카이제곱 수는 9.26, 자유도는 19 로써 카이제곱 분포에서 신뢰도가 95%이상이었다. 또한 poisson 분포 난수 생성은 composition 기법을 사용하였고, 마찬가지로 카이제곱 분포에서 신뢰도가 90%이상이었다.

그림 4 는 각 λ와 μ에 해당하는 적절한 인증벡터의 수를 box plot 으로 표기한 것이다. Box plot 은 25%-75%까지 표시하였고, x 는 1%와 99%를 표시한다. 또한 box plot 의 중심선으로 평균을, □ 은 중간값을 표시한다. 그림 8 에서 보듯이 일반적으로 통용되고 있는 m=5 값은 인증요청 rate 와 VLR 에 머무르는 시간 rate 이 비슷할 때 유효하다. 이 밖에 인증요청이 자주 일어나면 m 은 증가되어야 할 것이다.

그림 5 는 관련연구 및 3GPP AKA 와의 평균 인증지연시간을 비교한 것이다. 최적화된 *m* 값을 통해 사용자의 환경에 맞게 인증지연을 감소시킬 수 있다. 본 논문의 기법 사용 시 인증지연은 약 22.48 밀리초로 3GPP AKA 에 비해 약 50% 감소하였다. 또한 관련연구에 비해 각각 36%, 8% 성능을 향상시켰다.

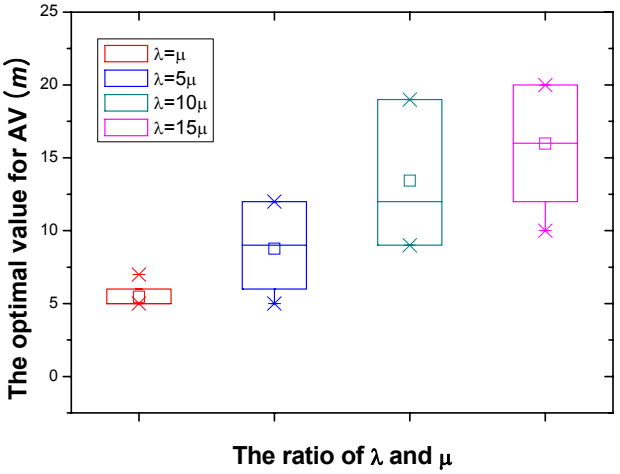

그림 4. 인증벡터의 적절한 단위

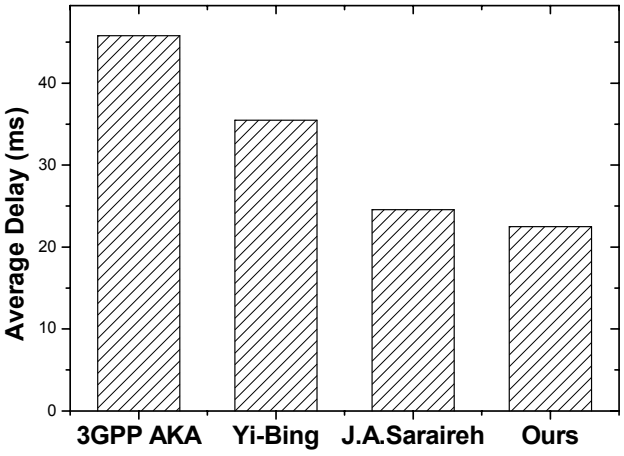

그림 5. 관련연구와의 평균 인증지연시간 비교

6. 결론

본 논문에서는 AKA 의 signaling load 를 수학적으로 분석하였고, 이를 통해 signaling load 에 영향을 미치는 요소를 파악하였다. AKA 의 인증벡터의 개수를 동적으로 선택하는 알고리즘을 제안하였고, 시뮬레이션을 통해 알고리즘의 우수성을 입증하였다.

참고문헌

[1] Third Generation Partnership Project, Technical Specification Group SA, 3G Security, "Security Architecture, version 4.2.0, Release 4", TS 33.102, 2001.

[2] Chung-Ming Huang, Jian-Wei Li, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption", *The 19th International Conference on Advanced Information Networking and Applications* (AINA), March 2005.

[3] Ja'afer Al-Saraireh and Sufian Yousef, "A New Authentication Protocol for UMTS Mobile Networks", *EURASIP Journal on Wireless Communications and Networking*, Issue 2, April 2006.

[4] Yi-Bing Lin, Yuan-Kai Chen, "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network", *IEEE Transactions on Wireless Communications*, Vol.2, No.3, May 2003.

[5] Ja'afer Al-Saraireh and Sufian Yousef, "Analytical model for authentication transmission overhead between entities in mobile networks," E*lsevier Computer Communications*, February 2007.