情報保護學會論文誌
第19卷 第2號, 2009. 4

3GPP 네트워크에서 효율적인 인증 데이터 관리를 위한 개선된 AKA 프로토콜*

김 두 환,† 정 수 환‡
숭실대학교 정보통신전자공학부

Improved AKA Protocol for Efficient Management of Authentication Data in 3GPP Network*

Doohwan Kim,† Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

본 논문에서는 3GPP 네트워크에서 USIM 기반의 사용자 인증 기법을 제안한다. 제안 기법은 기존의 3GPP 네트워크 접속을 위한 인증 방식에서 발생 가능한 Sequence Number 동기 문제, 인증 데이터 Overhead 문제, 네트워크 간 시그널링 Overhead 문제 등을 개선한다. 제안 기법은 기존의 USIM 기반의 AKA 인증 프로토콜을 기본 모델로 사용하고 단말과 SN이 공유한 SK와 Time Stamp를 통해서 AKA 인증 절차를 수행하도록 한다. 이렇게 함으로써 인증 벡터의 Sequence Number의 동기 여부를 확인할 필요 없이 Time Stamp 값으로 인증 벡터의 맵핑을 수행하여 Sequence Number 동기 문제를 해결할 수 있다. 뿐만 아니라 하나의 인증 벡터만을 관리하여 사용하기 때문에 SN에서의 인증 데이터 Overhead문제를 해결하고, SN과 HN 사이의 시그널링 Overhead 문제를 개선할 수 있다.

ABSTRACT

In this paper, we propose a USIM-based Authentication Scheme for 3GPP Network Access. The proposed scheme improves the problems of existing authentication protocol in 3GPP Network such as sequence number synchronization problem, the storage overhead of authentication data, and bandwidth consumption between Serving Network and Home Network. Our proposal is based on the USIM-based Authentication and Key Agreement Protocol that is defined in 3GPP Specification. In our scheme, mobile nodes share a SK with Serving Network and use a time stamp when mobile nodes are performing an authentication procedure with Serving Network. By using time stamp, there is no reason for using sequence number to match the authentication vector between mobile nodes and networks. So, synchronization problem can be solved in our scheme. As well as our scheme uses an authentication vector, the storage overhead of authentication data in Serving Network and bandwidth consumption between networks can be improved.

Keywords: EAP-AKA, 3GPP, Authentication

I. 서 론

3GPP 에서는 무선 네트워크상의 보안 문제점을 해결하기 위해 데이터의 무결성 및 기밀성을 제공하고 MS (Mobile Station)와 HN (Home Network) 사이의 상호인증을 지원하는 AKA 방식을 제안 하였다[1-3]. 하지만 3GPP-AKA 프로토콜에서는 SN

접수일(2008년 7월 25일), 수정일(2008년 10월 9일), 게재확정일(2008년 12월 10일)
* 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업 (2008-F-015-01, 서비스 가용성을 위한 이동성 관리 기술 연구)과 숭실대학교 교내연구비 지원에 의해 수행하였음.
† 주저자, shapja@cns.ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

(Serving Network)과 HN 사이의 Bandwidth Consumption 문제[4], SN에서 각 사용자에 대한 다수의 인증 벡터 (AV : Authentication Vector) 저장으로 인한 데이터 메모리 문제[5], Sequence Number 비동기로 인한 인증 실패 등의 문제점이 존재한다[6]. Huang은 이러한 문제를 해결하기 위해 SN이 HN으로부터 하나의 인증 벡터를 할당 받아 사용자 인증에 사용하도록 하여 SN과 HN 사이의 Bandwidth 소비량을 줄이는 프로토콜을 제안하였다. 그러나 위 기법은 MS의 이동 특성에 따라 인증 벡터의 동기 문제가 발생 가능하며 이러한 문제를 해결하기 위해서 MS는 SN에서 사용하였던 인증 정보를 지속적으로 저장해야 하는 문제점이 있다.

본 논문에서는 이러한 문제점을 해결하기 위해 Time Stamp 값을 사용하여 MS와 SN 사이의 인증 데이터 메모리 Overhead 및 인증 데이터 동기 문제를 해결하는 개선된 3GPP-AKA 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 프로토콜의 기본 동작 과정과 문제점을 분석한다. 3장에서는 제안하는 인증 기법의 동작 과정을 살펴본다. 4장에서는 기존의 3GPP-AKA 프로토콜과 제안하는 기법의 성능을 비교하고 5장에서 결론을 맺는다.

II. 관련 기술 및 문제점 분석

USIM (Universal Subscriber Identity Module)은 가입자의 ID 정보 등을 탑재한 SIM (Subscriber Identity Module)과 UICC (Universal IC Card)가 결합된 형태로 사용자 인증과 Global Roaming, 전자 상거래 등의 다양한 기능을 한 장의 카드에 구현한 것으로 3세대 통신 장비에 탑재되어 사용된다. USIM은 소형 CPU와 메모리를 가지고 있어 단말의 인증에 사용되는 암호 알고리즘과 프로세스를 동작한다. 또한 네트워크 서비스의 Profile 정보를 메모리에 저장하고 있어 금융, 신용, 교통카드 등의 기능을 수행할 수 있다.

본 장에서는 이러한 USIM을 탑재한 단말의 3GPP 네트워크 접속을 위한 인증 절차를 분석하고 기존의 USIM 기반 3GPP-AKA 인증 방식의 문제점 및 이를 개선하는 기법에 대해 살펴보도록 한다.

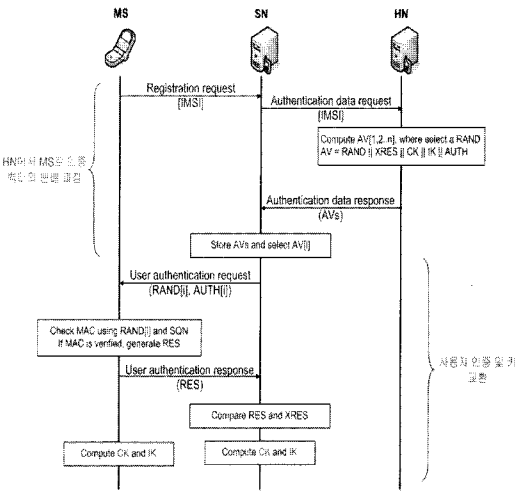
2.1 기존의 3GPP-AKA 프로토콜 동작 과정 및 문제점 분석

3GPP 네트워크 접속을 위해서는 USIM에 탑재된 AKA 인증 절차를 수행하여야 한다. AKA 인증은 크게 단말과 네트워크 사이의 인증 벡터 분배 단계와 분배된 인증 벡터와 USIM의 AKA 절차를 통한 인증 및 키 분배 단계로 나눌 수 있다. 위 두 절차가 끝나면 단말과 네트워크는 두 통신 객체 사이에 교환될 메시지의 무결성 및 기밀성 제공이 가능해진다. 또한 단말과 네트워크의 상호 인증을 통해 두 통신 객체간의 신뢰관계가 형성된다. [그림 1]은 3GPP 네트워크 접속 인증을 위한 전체 단계를 보여주며, 다음은 3GPP-AKA 인증 절차를 설명한 것이다.

2.1.1 3GPP-AKA 프로토콜 동작 과정

• 인증 벡터 분배 단계

1) SN에서 새로운 단말의 접근을 확인하면 단말의 ID인 IMSI (International Mobile Subscriber Identifier)를 요청하고 단말은 자신의 *IMSI*를 등록 요청 메시지에 포함하여 해당 SN에게 전달한다.
2) 등록 요청 메시지를 수신한 SN은 단말의 IMSI를 인증 요청메시지를 통해 HN에 전달한다.
IMSI를 수신한 HN은 해당 단말이 자신이 관리하는 단말인지 확인하고 확인 과정을 마치면 SN이 단말을 인증할 파라미터와 SN과 단말의 비밀통신을 위한 키를 생성하여 다수의 인증 벡터를 만든다. HN은 생성된 인증 벡터를 해당 SN에게 전송한다.



[그림 1] 3GPP-AKA 인증 절차

3) HN에게 해당 단말에 대한 다수의 인증 벡터를 수신한 SN은 이를 저장하고, 단말을 인증하기 위해 하나의 인증 벡터를 선택한다. 선택한 인증 벡터의 RAND와 AUTH만을 검출하여 단말에게 인증 요청 메시지를 통해 전달한다.

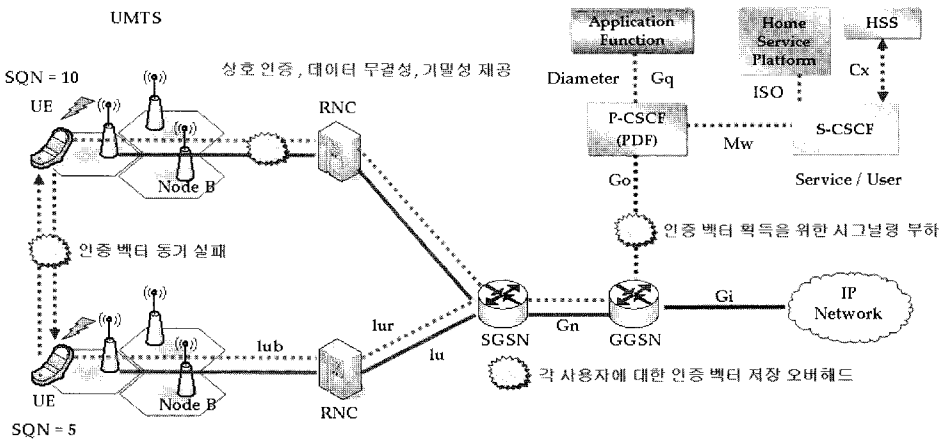
• 상호 인증 및 키 교환 단계

1) 인증 요청 메시지를 수신한 단말은 수신한 *RAND* 값과 자신의 마스터키를 이용하여 *AUTH*의 *MAC* 값을 확인한다. 이것이 확인되면 단말은 HN을 인증하여 수신한 인증 요청 메시지가 정상임을 알 수 있다. 이후 단말은 수신한 *AUTH*의 *SQN* 값이 적절한 범위의 값인지 확인하고 SN으로부터 인증 받기 위한 *RES* 값을 *RAND*와 마스터키를 사용하여 생성한다. 생성된 *RES* 값을 인증 응답 메시지에 포함하여 해당 SN에게 전달한다.
2) 인증 응답 메시지를 수신한 SN은 HN으로부터 수신한 인증 벡터의 *XRES* 값과 단말의 *RES* 값이 일치 하는지 확인하고 두 값이 일치하면 단말의 네트워크 접속을 허용한다.
3) 이후 단말과 네트워크 사이의 데이터 기밀성 및 무결성 제공을 위한 CK (Cipher Key)와 IK (Integrity Key)를 공유하게 된다. SN은 인증 벡터 내에 포함된 *CK*, *IK*를 사용하고 단말은 인증 요청 메시지에 포함된 *RAND* 값과 자신의 마스터키를 사용하여 *CK*, *IK*를 생성한다. 정상적인 인증 절차가 완료되면 SN의 *CK*, *IK*는 단말과 동일 한 값이 된다.

위 두 과정을 완료하면 단말과 3G 네트워크는 안전한 통신을 수행할 수 있다. 그러나 기존의 3GPP-AKA 인증 절차를 수행하는데 있어서 〔그림 2〕와 같은 몇 가지 문제점이 있다.

2.2.2 기존 AKA 프로토콜의 문제점 분석

- 인증 벡터 동기 문제: 단말이 이동한 SN에서 다시 이전의 SN으로 핸드오버 할 경우, 단말이 이동한 SN에서 사용한 인증 벡터의 Sequence Number가 핸드오버 한 SN의 Sequence Number 보다 큰 경우 잘못된 인증 벡터 동기로 인해 인증 실패 현상이 발생 가능하다.
- 인증벡터 획득을 위한 Bandwidth Consumption 문제: 다수의 단말이 하나의 SN에 오랫동안 머물러 있을 경우, 단말의 인증을 위한 인증 벡터 분배를 각 단말에 대해 여러 번 수행해야 한다. 이때 네트워크 간 인증 벡터 교환을 위한 다수의 Diameter 프로토콜 동작을 요구하게 되어 네트워크 노드 사이의 Bandwidth Consumption 문제가 발생한다.
- 각 사용자에 대한 인증 벡터 저장 문제: 3GPP 표준에서는 각 단말을 인증하기 위한 하나의 인증 벡터의 크기를 688 bits로 정의하고 있다. 하나의 단말에 대해 N 개의 인증 벡터를 할당할 경우, SN이 각 단말의 인증을 위해 저장해야 하는 인증 벡터 저장 공간은 총 688 Bit × N × R 이다. (N: 인증 벡터 수, R: 단말의 수) 따라서 다수의



〔그림 2〕 기존 3GPP-AKA 인증 방식의 문제점

단말이 SN에 존재할 경우, 단말의 핸드오버가 빈번하게 일어날 경우, 단말이 SN에 오랫동안 머물러 있을 경우 인증 벡터 저장을 위한 SN의 Storage Overhead가 발생 가능하다. 이러한 문제를 해결하기 위한 USIM 기반의 3GPP 인증 기술이 제안되고 있다. 다음은 이러한 인증 기술에 대한 설명이다.

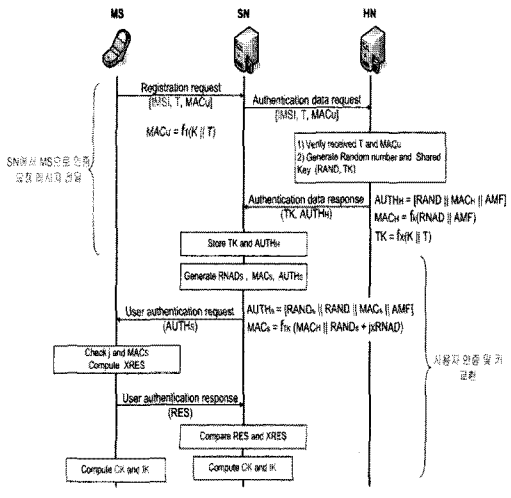
2.2 Huang et al.의 UMTS X-AKA 프로토콜 동작 과정 및 문제점 분석

2세대 통신 기술은 GSM 네트워크에서 사용자 인증을 위한 AKA 인증 방식은 단말과 네트워크 사이에 단방향 인증 문제로 인한 Impersonation Attack, False Base Station Attack 등의 문제점을 가지고 있다[7-10]. 이러한 문제점을 개선하는 3G 네트워크 인증 기술인 3GPP-AKA 인증 방식은 단말과 네트워크의 상호 인증 지원을 지원하고 단말과 네트워크가 공유한 무결성 키, 기밀성 키를 바탕으로 안전한 데이터 통신이 가능하다. 그러나 기존의 3GPP-AKA 인증 방식은 앞서 살펴본 바와 같이 다수 사용자 인증 수행을 위한 SN과 HN 사이에 Bandwidth Consumption 문제, 인증 데이터 Storage Overhead 문제, 인증 벡터의 Sequence 비동기로 인한 인증 실패 문제 등이 존재한다. Huang et al.은 이러한 세 가지 문제점을 개선하는 UMTS X-AKA 인증 방식을 제안하였다. UMTS X-AKA 방식에서는 단말과 네트워크가 공유한 K와 암호 알고리즘을 통해 AKA 프로토콜을 동작하게 한다. 기존의 3GPP-AKA 방식과 차이점은 인증 벡터의 동기를 *Sequence Number*가 아닌 *Index*를 사용한다는 점과 단말과 SN사이에 Temporary Key (TK)를 공유하여 단말과 SN이 AKA 프로토콜을 동작한다는 점이다. UMTS X-AKA 방식에서는 메시지 인증 코드 생성을 위한 f1, f2 암호 알고리즘과 키 생성 함수 f3, f4, fx를 사용한다[11,12]. 따라서 기존의 3GPP-AKA 방식에서 Sequence 비동기로 인한 재 인증 함수 f1*, f5*가 필요로 하지 않는다. 또한 기존의 f5 함수에서는 48 bit 키를 이용한 해시 알고리즘을 사용하지만 제안 기법에서 128 bit 연산의 fx 함수를 사용함으로써 강화된 보안을 제공한다. 제안 기법은 3GPP-AKA 방식과 동일하게 키 분배 과정과 인증 및 키 교환 과정으로 나누어 실행된다.

2.2.1 UMTS X-AKA 프로토콜의 동작 과정

• 등록 및 인증 벡터 분배 단계

1) 우선 [그림 3]과 같이 단말이 SN으로 *Registration Request* 메시지를 전달한다. *Registration Request* 메시지에는 단말의 *IMSI*, *T* (Time Stamp), *MACu* 값이 포함된다. *T*는 Replay 공격을 차단하고 단말과 네트워크 사이에 공유하는 *CK* (Cipher Key), *IK* (Integrity Key)의 Freshness를 제공하는데 사용된다.
(MACu = f1k(T))
2) SN은 *Registration Request* 메시지를 송신한 단말의 HN으로 *Authentication Data Request* 메시지를 전송한다. 이 메시지는 *Registration* 메시지와 동일한 파라미터를 가진다.
3) *Authentication Data Request* 메시지를 수신한 HN은 *T*값과 *IMSI*에 해당하는 *K*를 이용하여 수신한 메시지의 *MAC* 값을 검증한다. 검증이 확인되면 HN은 *T*값과 *K*를 이용하여 단말과 SN이 사용할 *TK*를 생성한다. 이 후 HN은 *RAND*와 MAC_H, *AMF* (Authentication Management Field), $AUTH_H$를 생성하고 이 값을 *TK*를 포함하여 SN에게 전달한다. MAC_H의 생성 방식은 3G 표준과 동일하다.



[그림 3] UMTS X-AKA 인증 절차

(TK = fxk(T), $AUTH_H$ = RAND || MAC_H || AMF)

4) HN으로부터 단말의 인증을 위한 *TK*, *RAND*, $AUTH_H$를 수신한 SN은 해당 파라미터를 저장하고 인증 및 키 교환 단계를 수행한다.

• 인증 및 키 교환 단계

1) HN으로부터 수신한 인증 파라미터를 기반으로 SN은 MS를 인증 하고 무결성 및 기밀성 키를 공유하기 위한 절차를 수행한다. 우선 SN은 *Random Number* $RAND_S$를 생성하고 이 값을 바탕으로 MAC_S를 생성한다. 그 후, 단말과 AKA 동작을 위한 $AUTH_S$를 생성하여 $RAND_S$와 $AUTH_S$를 단말에 전송한다. *(MAC_S = f^1_{TK}(MAC_H || $RAND_S$ + j*RAND), $AUTH_S$ = MAC_S || $RAND_S$ || RAND || AMF)*

2) 단말은 SN과 HN을 모두 인증하기 위해서 MAC_S 값을 검증한다. MAC_S에는 HN이 생성한 MAC_H 이 존재하기 때문에 MAC_S를 검증하면 SN과 HN 모두를 인증 할 수 있다. MAC_S가 올바르면 *jth index*를 검사하여 해당 요청 메시지가 재전송 된 것인지, 올바르게 수신된 것인지를 확인하고 $AUTH_S$로부터 *RAND*와 *AMF* 값을 획득한다. 검증이 완료되면 단말은 *RES*를 생성하여 SN에 전송하고 SN은 공유된 *TK*로 *XRES*를 생성하여 단말로부터 수신한 *RES*를 비교한다. 성공적인 검증이 완료되면 단말은 *TK*와 $RAND_S$를 이용하여 *CK*와 *IK*를 생성하고 단말과 공유한다. *($XRES = f^2_{TK}(RAND_S)$, $CK = f^4_{TK}(RAND_S)$, $IK = f^3_{TK}(RAND_S)$).*

2.2.2 UMTS X-AKA 프로토콜의 문제점 분석

UMTS X-AKA 방식은 단말과 SN이 공유한 *TK*를 사용하여 SN이 HN과 지속적인 통신 없이도 단말을 인증할 수 있다. 또한 SN이 HN으로부터 하나의 인증 벡터만을 할당 받아 사용하기 때문에 SN에서 단말의 인증을 위한 데이터 저장 공간도 줄여줄 수 있다. 그러나 UMTS X-AKA 방식은 단말의 이동 특성에 따라서 *jth index*가 SN과 맞지 않아 동기 문제로 인한 인증 실패 현상이 발생 가능하다. 이렇게 되면 MS는 HN으로부터 Full 인증 절차를 수행해야 한다. 또한 단말이 다른 SN으로 핸드오버 할 경우, 이전의 SN과 현재 SN사이에 인증 파라미터 교환이 되지 않기 때문에 HN으로 Full 인증 절차를 수행해야 한다.

III. 제안하는 3GPP-AKA 프로토콜

본 장에서는 3G 네트워크 접속 인증 방식에서 Sequence Number 비동기로 인한 인증 실패 현상과 SN에서 사용자 인증 데이터를 효율적으로 관리할 수 있는 개선된 3GPP-AKA 인증 방식에 대해 설명한다. 다음 〔표 1〕은 제안 기법에서 사용하는 주요 용어들을 정리하였다.

제안 기법에서 단말은 네트워크로부터 접속 인증을 수행하기 위해 자신의 현재 시간 값을 *Time Stamp* 파라미터와 이를 이용한 *MAC* 값을 생성하여 인증 요청 메시지를 통해 HN에 전송하게 된다. HN은 수신한 인증 요청 메시지의 *Time Stamp*와 *MAC* 값을 단말과 HN이 공유한 키로 검증하여 인증을 수행한다. 따라서 기존 *Sequence Number*의 동기 여부를 확인하지 않고 현재 시점에서 네트워크가 수신한 인증 요청 메시지가 정당한지를 *Time Stamp*를 이용하여 판별하기 때문에 기존 방식에서의 인증 비동기 현상을

〔표 1〕 주요 용어 정리

용 어	내 용
Time Stamp	단말의 현재 시간 값 T_i
SN	Serving Network
HN	Home Network
SK	Session Key, 단말과 SN 간에 생성되는 세션키
CK	Cipher Key, 단말과 네트워크 사이의 데이터의 기밀성을 제공하는 키
IK	Integrity Key, 단말과 네트워크 사이의 무결성을 제공하는 키
LAI	Location Area Identity, SN의 지역 ID
IMSI	International Mobile Subscriber Identifier로 단말의 ID
RADN	인증 서버에서 생성하는 임의의 수
AUTH	Authentication Value, 인증 서버에서 생성하는 인증 값
f1, f2	암호 알고리즘
f3, f4, fx	키 생성함수

개선할 수 있다. 또한 *Time Stamp* 값을 이용하여 매 인증 요청이 발생할 때마다 단말과 SN이 새로운 *SK, CK, IK*를 생성하여 Key Freshness를 제공할 수 있다. Bootstrapping 인증 시, SN은 HN으로부터 하나의 인증 벡터만을 할당 받아 사용하고 추가적인 HN과의 통신 없이 지속적으로 단말과 SN간에 AKA 프로토콜을 가능하게 함으로써 SN과 HN사이의 Bandwidth Consumption 문제를 해결할 수 있다. 뿐만 아니라 SN에서 사용자 인증을 위한 저장해야할 파라미터를 줄여 SN이 각 단말의 인증을 위해 저장해야할 메모리 용량을 개선하였다. 핸드오버 시에는 단말이 SN에서 새로운 SN으로 이동할 경우 Security Context Transfer (SCT) 방식을 사용하여 빠른 핸드오버 인증을 지원할 수 있다. 다음은 제안하는 3GPP-AKA 방식에 대한 설명이다.

3.1 Bootstrapping Authentication

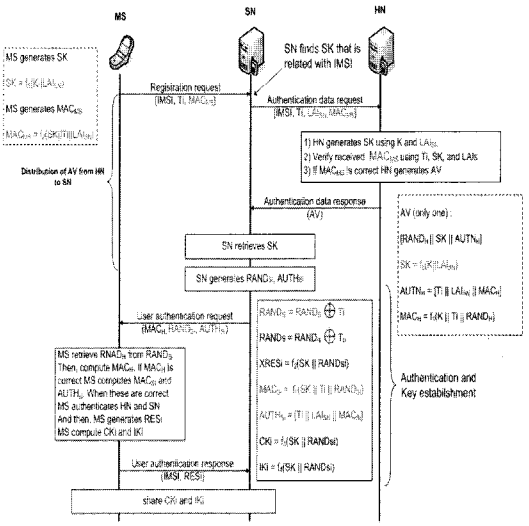
첫 번째, Bootstrapping 인증 절차는 기존의 3GPP-AKA 방식과 동일하게 사용자 등록 단계와 인증 및 키 교환 단계로 구성된다. *Time Stamp*와 단말이 HN과 공유한 K를 사용하여 단말과 SN이 AKA 동작을 수행하기 위한 *SK*를 생성 및 공유하고, 인증 요청 시마다 새로운 *Time Stamp*를 단말이 SN에 전송하여 새로운 인증 파라미터를 생성한다. 이렇게 함으로써 인증 벡터 동기 문제 및 SN과 HN 사이의 Bandwidth Consumption 문제 등을 해결할 수 있다. 다음은 제안 기법의 Bootstrapping Authentication 과정에 대한 설명이다.

• 등록 및 인증 벡터 분배 단계

1) 단말이 새로운 SN으로 접속하면 해당 SN의 LAI (Location Area Identity)와 *K*를 이용하여 단말과 SN이 지속적으로 사용할 *SK*를 생성한다. 이후 단말은 *Time Stamp*와 *MAC* 값을 생성하여 SN에 *Registration Request* 메시지를 전달한다.
($SK = f^5_K(LAI_{SN})$, $MAC_{MS} = f^2_K(SK \mid\mid T_i \mid\mid LAI_{SN})$
2) SN은 *Registration Request* 메시지를 송신한 단말의 HN으로 *Authentication Data Request* 메시지를 전송한다. 이 메시지는 *Registration* 메시지의 파라미터와 SN의 *ID*를 포함한다.
3) *Authentication Data Request* 메시지를 수신한 HN은 *LAI*값과 *IMSI*에 해당하는 *K* 값을 사용하여 단말과 SN이 공유할 *SK*를 생성하고, *T* 값과 *K*를 이용하여 수신한 메시지의 *MAC* 값을 검증한다. *MAC* 값이 검증되면 HN은 $RAND_H$와 MAC_H, $AUTH_H$를 생성하고 이 값에 *SK*를 포함하여 SN에게 전달한다.
($AUTH_H = T_i \mid\mid LAI_{SN} \mid\mid MAC_H$, $MAC_H = f^1_K(K \mid\mid T_i \mid\mid RAND_H)$)
4) HN으로부터 단말의 인증을 위한 *SK*, $RAND_H$, $AUTH_H$를 수신한 SN은 해당 파라미터를 저장하고 인증 및 키 교환 단계를 수행한다.

• 인증 및 키 교환 단계

1) HN으로부터 수신한 인증 파라미터를 기반으로 SN은 MS를 인증 하고 무결성 및 기밀성 키를 공유하기 위한 절차를 수행한다. 우선 SN은 $RAND_S$를 생성하고 *SK*, T_i 값을 바탕으로 MAC_S를 생성한다. 그 후, 단말과 AKA를 위한 $AUTH_S$를 생성하여 $RAND_S$, $AUTH_S$, MAC_H를 단말에 전송한다.
($RAND_{Si} = RAND_S \oplus T_i$, $RAND_S = RAND_S \oplus T_0$, $MAC_{Si} = f^1_{SK}(T_i \mid\mid RAND_{Si})$, $AUTH_{Si} = T_i \mid\mid LAI_{SN} \mid\mid MAC_{Si}$)
2) 단말은 SN과 HN을 모두 인증하기 위해서 MAC_H, MAC_S 값을 검증한다. MAC_H,



〔그림 4〕 제안하는 3GPP-AKA 인증 기법

MAC_S가 올바르면 단말은 RES를 생성하여 SN에 전송하고 SN은 공유된 SK로 $XRES$를 생성하여 단말로부터 수신한 RES를 비교한다. 성공적인 검증이 완료되면 단말은 SK와 $RAND_S$를 이용하여 CK와 IK를 생성하고 단말과 공유한다.

$(XRES = f^2_{SK}(RAND_{Si}),\ CK = f^4_{SK}(RAND_{Si}).\ IK = f^3_{TK}(RAND_{Si}))$

3.2 Handover Authentication

두 번째, 핸드오버 인증 기법에서는 단말이 다른 SN으로의 이동을 감지하면 새로운 SN에게 단말이 KTM (Key Transfer Material)을 전송하여 새로운 SN과 새로운 SK를 공유할 수 있다. 따라서 기존의 3GPP-AKA 방식과 같은 SCT 기반의 핸드오버 인증 파라미터 전달을 통해서 빠른 인증이 가능하다. 앞서 제시한 기존 3GPP-AKA 인증 방식의 문제점을 개선하기 위한 여러 기법들은 단말이 새로운 SN으로 핸드오버 할 때 단말과 SN이 세션 키를 공유하기 위해서는 반드시 HN으로의 통신이 필요로 하게 되므로 핸드오버 인증 지연이 발생 가능하지만 제안 기법에서는 이를 효율적으로 개선하였다.

• 새로운 SK 분배 단계

1) 단말이 새로운 SN으로 이동한 경우 단말은 새로운 SN과 SK를 공유해야만 AKA 인증 절차를 수행할 수 있다. 단말은 새로운 SN과 공유할 SK를 생성하고 SK를 안전하게 새로운 SN에게 전달하기 위해 KTM (Key Transfer Material)을 생성하여 새로운 SN에게 전달한다. *Registration Request* 메시지에는 단말의 *IMSI, Time Stamp, MAC, KTM*이 포함되어 전달된다.

$(SK_N = f^5_K(LAI_{SN\_NEW}),\ MAC_{MS} = f^2_K(SK_{old} \mid\mid T_i \mid\mid LAI_{SN\_NEW}),\ KTM = CK \oplus IK \oplus SK_N)$

2) SN은 해당 *IMSI*에 대한 SK를 찾고 SK가 존재하지 않으면 단말이 이전에 접속하였던 SN에게 *User Identity Request* 메시지를 전송한다. 해당 메시지에는 단말의 *IMSI*, 새로운 SN *ID, Time Stamp, MAC* 값이 포함된다.

3) 해당 메시지를 수신한 SN은 메시지에 포함된 *MAC* 값을 검증하여 정상적인 사용자임을 확인하고, 단말과 마지막에 공유하였던 무결성 및 기밀성 키를 찾는다. 해당키와 $RAND_H$를 포함한 *Authentication Data Response* 메시지를 현재 SN에 전달한다.

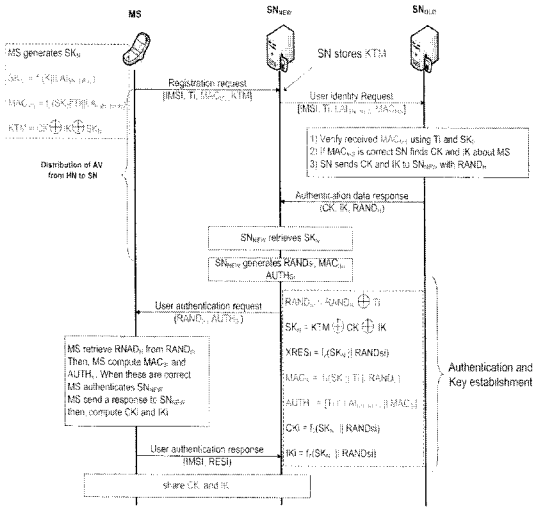
• 인증 및 키 교환 단계

1) SN은 *Authentication Data Response* 메시지를 수신하면 해당 CK와 IK를 이용하여 KTM을 XOR 연산하여 단말이 전송한 SK를 획득한다. 이후 단말은 $RAND_H$를 사용하여 $RAND_S$를 생성하고 이를 이용하여 MAC_S, $AUTH_S$, $XRES$를 생성한다. 이후 SN은 $RAND_S$와 $AUTH_S$를 *User Authentication Request* 메시지를 통해 단말에 전달한다.

$(SK_N = KTM \oplus CK \oplus IK,\ RAND_{Si} = RAND_H \oplus T_i,\ MAC_{Si} = f^1_{SK\_N}(T_i \mid\mid RAND_{Si}),\ AUTH_{Si} = T_i \mid\mid LAI_{SN\_NEW} \mid\mid MAC_{Si})$

2) 단말은 SN을 인증하기 위해서 MAC_S 값을 검증한다. MAC_S가 올바르면 단말은 RES를 생성하여 SN에 전송하고 SN은 공유된 SK로 $XRES$를 생성하여 단말로부터 수신한 RES를 비교한다. 성공적인 검증이 완료되면 단말은 SK와 $RAND_S$를 이용하여 CK와 IK를 생성하고 단말과 공유한다.

$(XRES = f^2_{SK\_N}(RAND_{Si}),\ CK = f^4_{SK\_N}(RAND_{Si}).\ IK = f^3_{SK\_N}(RAND_{Si}))$



〔그림 5〕 제안 기법의 핸드오버 인증 절차

IV. 제안 기법 성능 비교 및 분석

본 논문에서는 기존의 3GPP-AKA 인증 방식에서 발생 가능한 문제점을 분석하였고 이를 개선하는 다양한 인증 기법에 대해 살펴보았다. 그러나 단말의 이동성이 높은 현재 네트워크 환경에서 앞에서 살펴본 인증 기법들은 *Sequence Number* 비동기로 인한 인증 실패 현상과 SN에서 사용자 인증 데이터의 Overhead가 존재함을 확인하였다. 이를 해결하기 위해 본 논문에서는 *Time Stamp*와 단말과 SN이 공유한 *SK*를 이용한 개선된 3GPP-AKA 인증 기법을 제안하였다. 본 장에서는 제안 기법의 장, 단점 및 성능을 분석한다.

• 장 점

제안 기법에서는 기존의 인증 방식에서 *Sequence Number* 비동기로 인해 발생 가능한 인증 실패현상을 *Time Stamp* 값을 이용하여 해결하였다. 또한 단말과 SN사이에서 AKA 인증 프로토콜을 수행하므로 인증 벡터의 재획득 없이 단말과 SN사이에서 지속적인 인증 절차를 수행하고 새로운 암호 키를 생성할 수 있다. 또한 다수의 인증 벡터를 HN으로부터 할당 받는 대신 단말과 SN사이에 공유한 *SK*와 *Time Stamp*를 이용하여 지속적인 네트워크 접속 인증을 수행할 수 있으며, SN에서의 인증 벡터 저장 공간을 개선한다. 이렇게 함으로써 SN과 HN사이에서는 단말의 인증을 위한 별도의 시그널링 Overhead가 줄어들 수 있다.

• 단 점

제안 기법이 실제 네트워크 환경에 적용될 경우, SN에서 AKA 인증 프로토콜 동작을 위한 프로세스 Overhead가 존재한다. 기존의 3GPP 표준에서는 HN으로부터 할당받은 인증 벡터를 큰 계산량 없이 확인하는 절차만 거치고 단말의 인증을 수행하지만, 제안 기법에서는 SN에서 인증 벡터를 생성하고 검증 및 키 생성을 해야 하므로 Overhead가 존재한다. 또한 단말이 SN과의 지속적인 인증 프로세스를 위해서 *Time Stamp*, *SK*, *RAND* 값 등을 저장해야 하므로 단말의 저장량이 다소 증가한다.

4.1 기존 방식과 제안 기법의 비교 분석

다음 [표 2]는 기존의 3GPP 네트워크 접속 인증 기술과 제안하는 인증 기술에 대한 Sequence Problem, 인증 데이터 메모리 측면, 시그널링 Overhead 측면 등을 비교하여 정리하였다.

우선 제안 기법에서는 단말의 인증 수행 시 기존이 인증 방식과 달리 인증 벡터의 동기를 단말이 네트워크에 전송한 *Time Stamp* 값을 통해서 맵핑시키기 때문에 단말과 네트워크 사이에 Sequence Problem을 개선할 수 있다. 기존의 3GPP-AKA와 UMTS X-AKA는 단말과 네트워크 사이에 AKA 프로토콜 동작 시 *Sequence Number* 또는 *Index*를 비교 검사해야 하므로, 단말이 현재 SN에서 다른 SN으로 이동한 후 다시 이전의 SN으로 되돌아 올 경우, 또는 단말이 지속적으로 SN을 이동할 경우 인증 벡터의 비동기 문제가 발생하여 인증 실패현상이 발생할 수 있다. 제안 기법에서는 단말의 네트워크 접속 인증이 필요할 때 마다 단말에서 생성한 *Time Stamp*를 네트워크에 전송하여 그 값을 인증 벡터의 맵핑에 사용하기 때문에 별도의 인증 벡터 동기 검사를 할 필요가 없이 해당 *Time Stamp*를 이용한 인증 벡터 값의 일치 여부만 확인하면 되기 때문에 인증 벡터의 동기 문제를 개선할 수 있다.

인증 데이터의 메모리 측면에서도 제안 기법에서는 기존의 인증 방식보다 개선된 효과를 보인다. 단말, SN, HN은 네트워크 접속 인증을 수행하여 상호인증 및 키 교환을 위해 다양한 인증 요소들을 저장해야 한다. 특히 SN에서는 이동성이 많은 단말, 또는 지속적으로 SN에 머물러 있는 단말이 존재할 경우, 인증 데이터 관리를 위해 많은 데이터 저장 공간이 필요로 하다. [표 2]에서 살펴볼 수 있듯이, 제안 기법은 단말에서 저장해야할 인증 파라미터가 기존 표준 보다는 많지만 그 증가량이 매우 미흡하기 때문에 충분히 고려할만 하며, SN에서 각각의 단말을 인증하기 위해 저장해야할 데이터 저장 공간은 다른 방식에 비해 크게 개선되었다. 제안 기법에서는 사용자의 인증이 필요할 경우에만 단말과 SN이 공유한 SK와 *Time Stamp* 값으로 AKA 프로토콜을 수행하기 때문에 HN으로의 별도 인증 정보 요청 및 관리 없이 지속적으로 단말의 네트워크 접속 인증을 관리할 수 있기 때문에 효율성이 크다. 단말 및 SN에서 저장해야 하는 인증 파라미터는 *RANDs*, *MACs* 값이 새롭게 추가되었지만, 기존 표준과 달리 하나의 인증 벡터만을 관리하므로 저장 공간 측면에서 효율적이다.

마지막으로 Sequence Problem으로 인해 발생하는 단말과 네트워크의 시그널링 Overhead 측면과 단말이 SN을 핸드오버 할 경우 단말과 네트워크의 시

〔표 2〕 제안 기법 성능 비교

비교 항목		3GPP AKA	UMTS X-AKA	제안 기법
Sequence Problem		Yes	Yes	No
인증 데이터 메모리 용량 *N : 인증 벡터 수 *R : MS 수	MS	560 bits	768 bits	724 bits
	SN	(688 × N) × R bits	896 × R bits	852 × R bits
	HN	(688 × N) × R bits	336 × R its	320 × R bits
저장되어야 할 인증 파라미터	MS	RAND, CK, IK, SQN, AK, AMF, MAC	$RAND_S$, RAND, MAC_H, MAC_S, CK, IK, TK	$RAND_S$, MAC_S, CK, IK, SK, T_i
	SN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	$RAND_S$, RAND, MAC_H, MAC_S, CK, IK, TK, XRES	$RAND_S$, MAC_S, CK, IK, SK, T_i, XRES
	HN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	RAND, MAC_H, TK, AMF	RAND, MAC_H, SK
시그널링 Overhead	Sync. Failure (재인증 요청)	5 + 2a (a 〈1)	5	x
	Handover (SN 간)	3 + 2b (b 〈a)	3 + 2a (HN 과 Full 인증 재 수행)	3 + 2b (b 〈a)
계수 정의	1 : MS와 SN 사이의 signaling cost a : SN과 HN 사이의 signaling cost b : SN과 SN 사이의 signaling cost			
인증 데이터 별 저장 공간	RAND : 128 bit, XRES : 128 bit, CK : 128 bit, IK : 128 bit, SQN : 48 bit, AK : 48 bit, AMF : 16 bit, MAC : 64 bit			

그널링 Overhead 측면에서 제안 기법이 기존 방식보다 효율적임을 알 수 있다. 기존 3GPP 표준에서 단말과 네트워크 사이에 *Sequence Number*의 비동기 현상이 발생할 경우 단말은 Re-synchronization 절차를 수행해야 하기 때문에 단말과 네트워크 사이에 시그널링 Overhead가 발생 가능하다. UMTS X-AKA 방식에서도 단말이 HN으로 재 인증 요청을 수행해야 하기 때문에 별도의 HN과 시그널링이 필요로 하다. 또한 단말이 SN으로 핸드오버 할 경우 제안기법은 3GPP-AKA 프로토콜에서와 같이 Security Context Transfer를 사용하여 빠른 재인증이 가능하지만 UMTS X-AKA 방식에서는 HN과 다시 Full 인증을 수행하기 때문에 시그널링 Overhead가 존재한다.

결론적으로 제안 기법을 통해서 앞서 살펴본 기존의 3GPP-AKA 인증 방식에서 발생 가능한 인증 문제점에 대해서 개선된 효과를 보일 수 있으며, 기존 AKA 프로토콜의 암호 알고리즘과 동일한 프로세스를 가지는 인증 방식의 제안으로 기존 기술과의 호환성을 가진다.

V. 결 론

Ubiquitous 네트워크 환경에서 3GPP 이동 통신 네트워크는 넓은 사용자 서비스 영역과 Global Roaming을 지원하는 무선망으로 널리 사용되고 있다. 이러한 3GPP 네트워크를 접속하기 위해서는 USIM 기반의 AKA 인증 절차가 필수적으로 수행되어야 한다. 그러나 기존의 3GPP-AKA 인증 방식은 Ubiquitous 네트워크 환경에서 단말의 빠른 이동성 및 효율적인 인증 관리를 제공하는데 어려움이 존재한다. 따라서 기존의 3GPP 네트워크에서 발생 가능한 인증 문제를 개선할 필요성이 존재한다.

본 논문에서는 단말과 SN이 공유한 *SK*와 *Time Stamp* 값을 이용하여 기존의 3GPP 인증 방식에서 발생 가능한 인증 문제를 해결하는 개선된 3GPP-AKA 인증 프로토콜을 제안하였다. 현재 이동 통신 네트워크에서는 단말이 빠르고 빈번하게 네트워크 접속 지점을 변경하기 때문에 네트워크 접속 변경에 따른 접속 인증 시 인증 실패현상이 발생 가능하다. 제안 기법에서는 이러한 문제점을 *Time Stamp*를 이

용한 인증 데이터의 맵핑 기법을 통해 해결할 수 있기 때문에 기존의 3GPP 네트워크에서의 인증 기법보다 신뢰적인 인증 절차를 수행할 수 있다. 뿐만 아니라 단말기의 보급과 함께 네트워크에서 관리해야할 사용자 수의 증가로 네트워크에서 관리해야할 사용자 정보가 급격하게 증가하는 네트워크 환경에서는 제안 기법과 같이 사용자 인증 및 네트워크 접속 관리를 효율적으로 제공하는 인증 기법이 필수적이다.

참 고 문 헌

[1] 3GPP, "TSG services and system aspects, 3G security, security architecture (R5)," 3GPP TS 33.102 V5.5, 2004.

[2] 3GPP, "TSG services and system aspects, 3G security, formal analysis of the 3G authentication protocol, version 3.1.0," 3GPP TR 33.902, 1999.

[3] 3GPP, "TSG services and system aspects, 3G security, report on the evaluation of 3GPP standard confidentiality and integrity algorithm, version 1.1.0," 3GPP TR 33.909, 1999.

[4] C. Huang and J. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption," Proceedings of the 19th International Conference on Advanced Information Networking and Application 2005, pp. 392-397, Mar. 2005.

[5] W. Juang and J. Wu, "Efficient 3GPP authentication and key agreement with robust user privacy protection," Proceedings of the 2007 IEEE on Wireless Communications and Networking Conference, pp. 2720-2725, Mar. 2007.

[6] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communications, vol. 4, no. 2, pp. 734-742, Mar. 2005.

[7] L. Harn and H. Lin, "Modifications to enhance the security of GSM," Proceedings of the 5th National Conference on Information Security, Taipei, Taiwan, R.O.C, May 1995.

[8] C. Lee, M. Hwang, and W. Yang, "Enhanced privacy and authentication for the global system for mobile communications," Wireless Network, vol. 5, no. 4, pp. 231-243, July 1999.

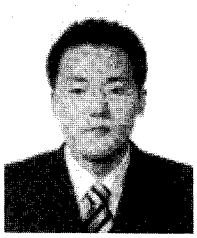
[9] H. Lin and L. Harnm, "Authentication protocols for personal communication System," ACM SIGCOMM Computer Communication Review, vol. 25, no. 4, pp. 256-261, Oct. 1995.

[10] ETSI. Recommendation gsm 02.09: Security related network functions. Technical report, European Telecommunications Standards Institute, ETSI, June 1993.

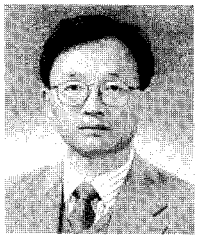
[11] I. Goldberg and D. Wagner, Architectural considerations for cryptanalytic hardware, Chapter 10 of Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design, O'Reilly, July 1998.

[12] P. Karger, Y. Frankel, and A. Herzberg, "Security issues in a CDPD wireless network," IEEE Personal Communication, vol. 2, no. 4, pp. 16-27, Aug. 1995.

〈著者紹介〉



김 두 환 (Doohwan Kim) 학생회원
2006년 2월: 숭실대학교 정보통신전자공학부 졸업
2008년 8월: 숭실대학교 정보통신공학과 석사
2008년 8월~현재: 삼성전자 정보통신총괄 통신연구소 엔지니어
〈관심분야〉 3G 네트워크 보안, VoIP 보안, DRM



정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 학사
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One SW Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 부교수
2009년 3월~현재: 지식경제부 지식정보보안 PD
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 네트워크 보안, RFID/USN 보안