한국산학기술학회논문지
Vol. 11, No. 12 pp. 5049-5057, 2010

3G 네트워크에서 프라이버시 보호를 강화한 효율적인 인증 메커니즘

전서관[1], 오수현[2*]
[1]한국시스템보증(주), [2]호서대학교 정보보호학과

An Efficient Authentication Mechanism Strengthen the Privacy Protection in 3G Network

Seo-Kwan Jeon[1] and Soo-Hyun Oh[2*]
[1]Korea System Assurance Co., Ltd., [2]Department of Information Security, Hoseo University

요 약 이동통신 기술 및 다양한 서비스 개발로 모바일 사용자들은 해마다 증가하고 있다. 그러나 무선 네트워크 환경에서 동작하는 모바일 서비스들은 불법적인 변조, 도청, 신분위장 등 다양한 보안위협에 노출되어 있다. 이에 따라 3GPP에서는 안전한 이동통신 서비스를 제공하기 위하여 인증과 키 동의를 수행하는 3GPP-AKA 표준을 제정하였다. 그러나 3GPP-AKA 프로토콜은 관련 연구들을 통해 sequence number 동기화 문제, false base station을 이용한 공격, 프라이버시 문제 등이 발견되었다. 따라서 본 논문에서는 3G 네트워크에서 프라이버시를 강화한 효율적인 인증 기법을 제안한다. 제안하는 인증 기법에서는 타임스탬프를 사용하여 기존의 3GPP 인증 방식에서 발견된 sequence number 동기화 문제를 해결하고, 비밀토큰을 이용하여 프라이버시 관련 문제를 해결하였다. 또한 하나의 인증벡터만을 사용하기 때문에 SN과 HLR 사이의 대역폭 소비 문제와 SN의 인증 데이터 오버헤드 문제를 개선할 수 있다.

Abstract As communication technologies are developed and variety of services to mobile devices are provided, mobile users is rapidly increasing every year. However, mobile services running on wireless network environment are exposed to various security threats, such as illegal tampering, eavesdropping, and disguising identity. Accordingly, the secure mobile communications services to 3GPP were established that the standard for 3GPP-AKA specified authentication and key agreement. But in the standard, sequence number synchronization problem using false base station attack and privacy problem were discovered through related researches. In this paper, we propose an efficient authentication mechanism for enhanced privacy protection in the 3G network. We solve the sequence number synchronization existing 3GPP authentication scheme using timestamp and strengthen a privacy problem using secret token. In addition, the proposed scheme can improve the bandwidth consumption between serving network and home network and the problem of authentication data overhead for the serving network because it uses only one authentication vector.

Key Words : 3GPP-AKA, Authentication, Privacy, IMSI, Security token

1. 서론

최근 이동통신 기술의 발달과 다양한 서비스들이 개발되면서 문자나 음성 서비스만을 제공하던 과거와는 달리 교통, 금융, 멀티미디어 서비스까지 그 영역을 확장해 나가고 있다. 그러나 모바일 서비스들은 무선 매체의 특성으로 인하여 불법적인 변조, 도청, 신분위장 등 다양한 보안위협에 노출되기 쉽다[9,10]. 이러한 보안 위협들에 대응하고 안전한 모바일 서비스 환경을 구축하기 위해서는 암호화 기능이나 사용자 인증 기법 등 보안 기술이 반드시 제공되어야 한다.

3GPP(3rd Generation Partnership Project)에서는 모바

*교신저자 : 오수현(shoh@hoseo.edu)
접수일 10년 09월 28일 수정일 (1차 10년 11월 03일, 2차 10년 11월 23일) 게재확정일 10년 12월 17일

일 환경에서 사용자 인증 및 암호화, 메시지 무결성 등을 제공하기 위해 3GPP-AKA(3GPP- Authentication and Key Agreement)라는 표준을 제정하였다[1-4]. 그러나 3GPP-AKA 프로토콜은 관련 연구들을 통해 몇몇 취약점들이 발견되었다. 대표적인 것으로 Zhang 등은 3GPP-AKA에서 사용하는 sequence number에 대한 동기 문제와 false base station을 이용한 공격이 가능함을 지적하였다[5,6]. 또한 Juang[7] 등은 단말의 영구 식별자인 IMSI (International Mobile Subscriber Identity)의 평문 전송으로 인한 프라이버시 문제를 제기하였고, Kim[11] 등은 다수의 인증벡터 사용으로 인한 인증 데이터 오버헤드 문제를 지적하였다.

본 논문에서는 3GPP-AKA 표준 프로토콜이 가지고 있는 보안 취약점들을 해결하고, Juang과 Kim등이 제안한 인증 기법을 개선하여 프라이버시를 강화하고 3G 네트워크에서 효율적으로 사용할 수 있는 개선된 인증 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 3GPP에서 제정한 표준 AKA 프로토콜의 기본 동작과 취약점을 분석하고, 이를 개선한 관련 연구들에 대해 기술한다. 그리고 3장에서는 기존의 프로토콜이 갖는 취약점을 해결하고 프라이버시를 강화한 개선된 인증 방식을 제안하고, 4장에서는 제안한 인증 기법의 안전과 효율성에 대해서 분석하고 마지막 5장에서 결론을 맺는다.

2. 관련연구

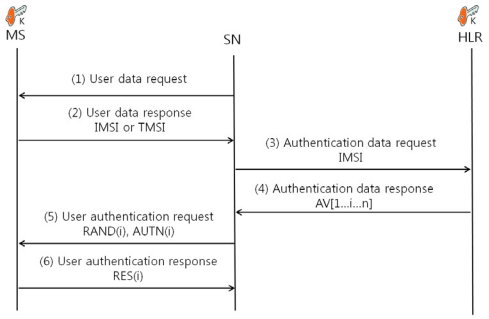
본 장에서는 3GPP-AKA 표준 프로토콜에 대한 기본 동작과 문제점에 대해서 알아보고 기존에 연구되었던 인증 기법들을 분석한다.

2.1 3GPP-AKA

3GPP에서는 모바일 사용자와 네트워크 간 상호인증과 키 분배를 위한 3GPP-AKA 프로토콜을 정의하였다. 3GPP-AKA 프로토콜의 네트워크 환경은 단말(MS ; Mobile station)을 소유한 사용자, 홈네트워크(HLR)와 단말을 연결하고 서비스를 제공하는 Serving Network(SN), 그리고 가입자에 대한 정보와 인증벡터를 관리하는 홈 네트워크로 구성된다. 3GPP-AKA에서는 단말과 홈 네트워크 사이에 사전 공유한 비밀키 K를 통해 SN과 단말과의 상호인증을 수행하고 이후 메시지 무결성 확인과 암호화를 위한 키 동의 과정을 수행한다[12].

그림 1은 3GPP-AKA 프로토콜의 인증 과정을 나타낸다. 먼저 단말이 SN의 영역에 접근하면 SN은 단말에게 사용자 인증요청 메시지를 보내고 단말은 이에 따른 응답으로 단말의 식별자 IMSI(International Mobile Subscriber Identity)나 TMSI(Temporary Mobile Subscriber Identity)를 전달한다. 여기서 TMSI는 단말의 임시 식별값으로써 초기 인증과정을 마친 후에 SN은 유일한 TMSI를 생성하여 동의된 암호화키를 이용해 암호화되어 단말에게 전달된다. 이러한 TMSI는 단말의 재인증 과정에서 IMSI를 보호하기 위해 사용된다. SN은 단말의 인증을 위해 HLR에게 단말의 영구 식별자인 IMSI를 전달하고 HLR은 IMSI에 대한 단말의 정보를 추출하여 사전 공유된 비밀 키 K와 HLR이 선택한 난수 RAND를 이용하여 n개의 인증벡터(AV)를 생성하여 SN에게 전송한다. 각 AV는 RAND, CK, IK, XRES, AUTN으로 구성되고 단말과 HLR이 공유하는 함수 f1, f2, f3, f4, f5에 비밀 공유 키 K와 RAND를 입력 값으로 다음과 같이 생성한다.

$$MAC=f1_K(SQN||RAND||AMF)$$
$$XRES=f2_K(RAND)$$
$$CK=f3_K(RAND)$$
$$IK=f4_K(RAND)$$
$$AK=f5_K(RAND)$$
$$AUTN=((SQN\oplus AK)||AMF||MAC)]$$



[그림 1] 3GPP-AKA 프로토콜

여기서 SQN은 인증벡터의 재사용을 막기 위한 카운터 값으로 SQN을 보호하기 위해 익명 키 AK로 XOR 연산된다. AMF는 인증관리 필드로 사업자가 규정할 수 있는 값이며 키의 주기, 암호화 방식 등을 정의할 수 있다. n개의 인증벡터를 전달받은 SN은 i번째 AV(i)를 선택하여 RAND(i),와 AUTN(i)를 단말에게 전송한다. 단말은 RAND(i)와 자신의 비밀 키 K를 통해 SQN을 검사하여 인증토큰이 재사용되었는지 판별한다. 이후 MAC값을 검

증함으로써 SN을 인증하고 RES(i)를 계산하여 SN에게 전송하고 SN은 XRES(i)와 전달받은 RES(i)를 비교하여 같은지 확인한 후 CK(i)와 IK(i)를 통해 비밀통신을 시작한다.

2.2 3GPP-AKA의 취약성 및 기존 연구

지금까지 다양한 관련 연구를 통해 제시된 3GPP-AKA 프로토콜의 보안 취약점은 다음과 같다.

- **SQN 동기화 문제** : 3G 네트워크 환경에서 단말이 이동한 SN에서 다시 이전의 SN으로 핸드오버 할 경우, 단말이 이동한 SN에서 사용한 인증벡터 SQN과 핸드오버 한 SN의 SQN의 비동기화로 인해 인증실패 현상이 발생할 수 있다.[8, 11]
- **False base station에 의한 공격** : Zhang 등은 false base station 장치를 이용한 Redirection Attack을 제시하였다[5]. Redirection Attack은 단말과 SN 사이의 통신에 개입하여 사용자가 의도하지 않은 다른 SN으로 redirect하는 공격이다. 이와 같은 공격의 원인은 단말과 SN 사이의 완벽한 상호인증이 제공되지 않기 때문에 발생할 수 있다.
- **SN과 HLR 사이의 대역폭 소비 문제** : 다수의 단말이 하나의 SN에 오랫동안 머물러 있을 경우, 단말의 인증을 위한 인증벡터 분배를 각 단말에 대해 여러 번 수행해야 한다. 이때 네트워크 간 인증 벡터 교환을 위한 다수의 Diameter 프로토콜 동작을 요구하게 되어 네트워크 노드 사이의 대역폭 소비 문제가 발생할 수 있다[8].
- **IMSI 평문 전송에 의한 프라이버시 문제** : Juang 등은 SN의 비정상적인 동작에 대해서 단말의 영구 식별자인 IMSI가 평문으로 전송되는 문제를 지적하였다. 이러한 IMSI의 노출로 인해 사용자의 신원이나 위치정보 등이 드러나는 프라이버시 문제가 발생할 수 있다.

(1) Juang 등의 인증 기법

3GPP-AKA 프로토콜에서는 단말의 재 인증이 요구되거나 단말의 핸드오버로 인한 인증이 요구될 때 사용자 신원 보호를 위해 단말의 임시 가입 식별자인 TMSI를 사용한다. 이 때 인증을 요청하는 SN이 TMSI에 대응되는 IMSI를 찾아낼 수 없으면 단말에게 IMSI를 요구하게 된다. 이때 전송되는 IMSI는 평문으로 전달된다.

Juang 등은 단말의 핸드오버 과정 중에 새로운 SNNew가 이전 SNOld를 찾을 수 없거나 이전 SNOld로부터 TMSI에 대한 정보를 찾을 수 없을 때 단말은 자신의 영구 식별자인 IMSI를 평문으로 전송하는 문제점을 발견하였다. 이러한 경우 IMSI는 단말의 고유 식별자인 IMSI 노출로 인해 사용자 프라이버시를 침해하 수 문제가 발생할 수 있다.

(2) Kim 등의 인증 기법

Kim 등은 3GPP 네트워크에서 USIM 기반의 사용자 인증 기법을 제안하였다. Kim 등이 제안한 인증 기법은 3GPP 네트워크워크 접속을 위한 인증 방식에서 발생 가능한 SQN 동기 문제, 인증 데이터 오버헤드 문제, 네트워크 간 시그널링 오버헤드 문제 등을 개선하였다.

Kim 등이 제안한 인증 기법은 기존의 USIM 기반의 AKA 인증 프로토콜을 기본 모델로 사용하고 단말과 SN이 공유한 세션키와 타임스탬프를 이용하여 AKA 인증 절차를 수행한다. 단말의 현재 시간 값인 타임스탬프를 이용하여 SQN의 동기 여부를 확인하지 않고 현재 시점에서 네트워크가 수신한 인증 요청 메시지가 정당한지를 판별하는 기법을 이용하여 인증 비동기 현상을 개선하였다. 또한 하나의 인증벡터만을 사용하여 AKA 절차를 수행하기 때문에 SN과 HLR 사이의 인증 데이터 오버헤드를 개선하였다. 그러나 Kim 등의 인증 기법은 단말과 SN 사이에 세션키를 갱신하기 위해서 HLR을 경유해야하기 때문에 세션 키 갱신에 따른 인증 지연이나 시그널링 오버헤드 문제가 발생할 수 있다. 또한 IMSI의 평문 전송으로 인한 프라이버시 문제도 여전히 남아 있다.

3. 제안하는 PE-AKA 프로토콜

본 장에서는 3G 네트워크 접속 인증 방식에서 Juang 등과 Kim 등이 제안한 인증기법을 개선하여 사용자 프라이버시를 강화하고 UMTS 환경에서 효율적으로 사용할 수 있는 PE-AKA(Privacy-Enhanced Authentication and Key Agreement) 프로토콜을 제안한다. 프로토콜 설명에 앞서 제안하는 프로토콜에서 사용하는 기호와 의미는 표 1과 같다.

[표 1] 표기법

기호	의미
IMSI	단말의 영구 가입 식별자
TMSI	단말의 임시 가입 식별자
x	HLR의 비밀 마스터 키
wi	비밀토큰
w'i+1	비밀토큰 갱신을 위한 마스킹 값

Ti	단말이 생성한 Time Stamp
LAI_A	A의 위치 식별자
RAND	난수
CK	암호화 키
IK	메시지 무결성 키
SK	단말과 SN이 공유하는 세션 키
MAC	메시지 인증 코드
RES	단말의 응답 값
XRES	기대된 응답 값
AMF	인증 관리 필드
$AUTN_A$	A의 인증토큰
$f1_K()$, $f2_K()$	64비트 출력을 갖는 메시지 인증 함수
$f3_K()$, $f4_K()$, $f5_K()$	128비트 출력을 갖는 키 생성 함수
⊕	XOR 연산

3.1 가정사항

제안하는 PE-AKA 프로토콜은 다음과 같은 가정 사항을 만족해야한다.

- HLR은 비밀키 K와 비밀토큰 $w_i=H(x||r_i)$, r_i를 생성하여 단말에 저장한다. 여기서 x는 비밀토큰을 생성하기 위해 HLR 만이 알고 있는 비밀 마스터 키이고 r_i는 i 번째 생성한 난수이다.
- 단말과 SN, HLR 사이에는 메시지 인증 코드와 키 생성을 위한 MILENAGE 알고리즘을 공유한다.
- SN과 HLR은 신뢰된 기관으로 SN이나 HLR의 제어권을 얻는 것은 불가능하며, SN과 HLR 사이의 통신은 안전한 채널을 이루고 있다고 가정한다.
- SN이 단말에게 평문으로 IMSI를 요구하는 경우에만 비밀토큰을 사용한다.

제안하는 프로토콜에서 사용하는 기호와 의미는 표 1과 같다.

3.2 제안하는 PE-AKA 프로토콜

본 논문에서 제안하는 프로토콜은 3가지 경우로 나누어 수행한다. 먼저 인증벡터를 분배받는 초기 인증 절차와 초기 인증 절차 이후 재인증이 요구될 때 수행하는 재인증 절차, 마지막으로 단말의 이동으로 인한 핸드오버시의 인증 절차로 나누어 설명한다.

(1) 초기 인증 과정

① 단말이 새로운 SN으로 접속하면 해당 SN의 LAI_{SN}와 비밀 키 K를 이용하여 세션키 SK를 생성한다. 이후 SN에 전달할 IMSI를 비밀토큰을 이용하여 $P_i= w_i⊕IMSI$를 계산한 후 타임스탬프 T_i 생성하여, MAC_{MS}를 계산하여 SN에게 P_i, T_i, r_i, MAC_{MS}를 전달한다.

$SK=f5_K(LAI_{SN}||T_i)$, $MAC_{MS}=f1_K(SK||T_i||LAI_{SN})$

② SN은 HLR에게 단말로부터 수신한 메시지에 자신의 위치 식별자를 포함하여 인증벡터 요구 메시지를 전달한다.

③ HLR은 자신의 마스터 키 x를 이용하여 $w_i=H(x||r_i)$을 계산하여 P_i로부터 IMSI를 복구한 후 이에 대응되는 비밀 키 K를 찾아 LAI_{SN}을 이용해 세션키 SK를 계산한다. 이후 MAC_{MS}를 검증하여 검증이 성공적으로 이루어지면 비밀토큰 값인 갱신을 위하여 난수 r_{i+1}을 생성하여 다음에 사용될 비밀토큰 w_{i+1}계산하고, 단말에게 안전하게 전송하기 위해 w'_{i+1}값으로 마스킹 한다. 이후 HLR은 난수 $RAND_H$를 생성하여 단말과 SN사이의 인증 및 키 교환 절차에 사용될 하나의 인증벡터 AV를 생성하여 인증 데이터 응답 메시지로서 IMSI, AV, w'_{i+1}, r_{i+1}을 SN에게 전송한다.

$w_{i+1}=H(x||r_{i+1})$

$w'_{i+1}=H(K||r_{i+1})⊕w_{i+1}$

$AV=(RAND_H||SK||AUTN_H)$

$AUTN_H=(AMF||T_i||MAC_H)$

$MAC_H=H(AMF||r_{i+1}||w'_{i+1}||RAND_H||T_i||K||SK)$

$SK=f5_K(LAI_{SN}||T_i)$

④ 인증벡터를 전달받은 SN은 인증벡터를 자신의 데이터베이스에 저장한다. SN은 난수 $RAND_{SN}$를 생성하여 공유된 SK를 이용하여 단말과 AKA 절차를 위한 $AUTN_{SN}$를 생성한다. SN은 사용자 인증 요구 메시지로서 $AUTN_{SN}$, $RAND_{SN}$, w'_{i+1}, r_{i+1}를 포함하여 단말에게 전달한다.

$RAND_{SN}=RAND_H⊕T_i$

$AUTN_{SN}=(AMF||MAC_H||MAC_{SN})$

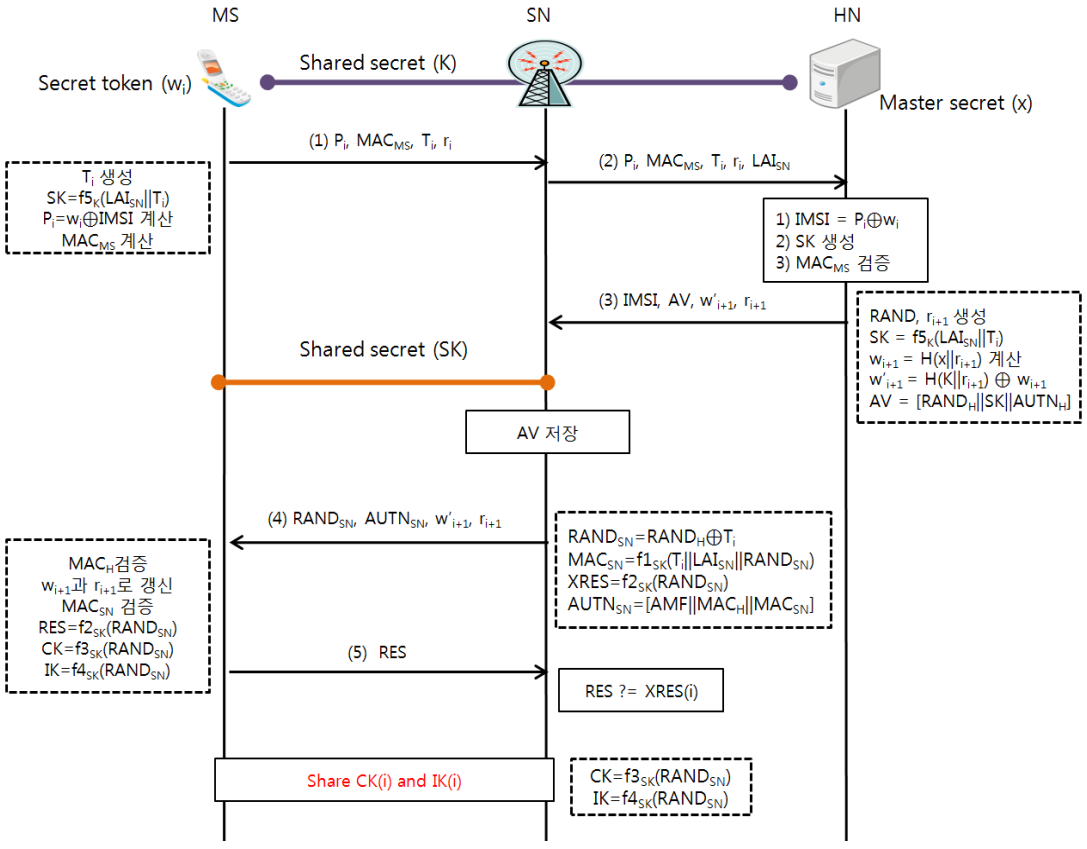
$MAC_{SN}=f1_{SK}(T_i||LAI_{SN}||RAND_{SN})$

⑤ 사용자 인증 요청 메시지를 수신한 단말은 $RAND_{SN}$로부터 RAN_{DH}를 계산하여 MAC_H를 검증한다. 검증이 성공적으로 이루어지면 $w_{i+1}=w'_{i+1}⊕H(K||r_{i+1})$을 계산하여 비밀토큰을 갱신한다. 이후 MAC_{SN}를 검증하고 검증이 성공적으로 이루어지면 단말은 사용자 인증 응답 값으로써 RES를 계산하여 SN에 전달한다. 메시지 전송 중에 단말은 비밀통신을 위한 CK와 IK를 계산할 수 있다.

$CK=f3_{SK}(RANS_{SN})$

$IK=f4_{SK}(RAND_{SN})$

$RES=f2_{SK}(RAND_{SN})$



[그림 2] PE-AKA 초기 인증 절차

⑥ 사용자 인증 응답 메시지를 전달 받은 SN은 XRES를 계산하여 수신한 RES와 비교하여 일치하면 단말을 인증하고 CK와 IK를 생성하여 비밀 통신을 수행한다.

(2) 재 인증 과정

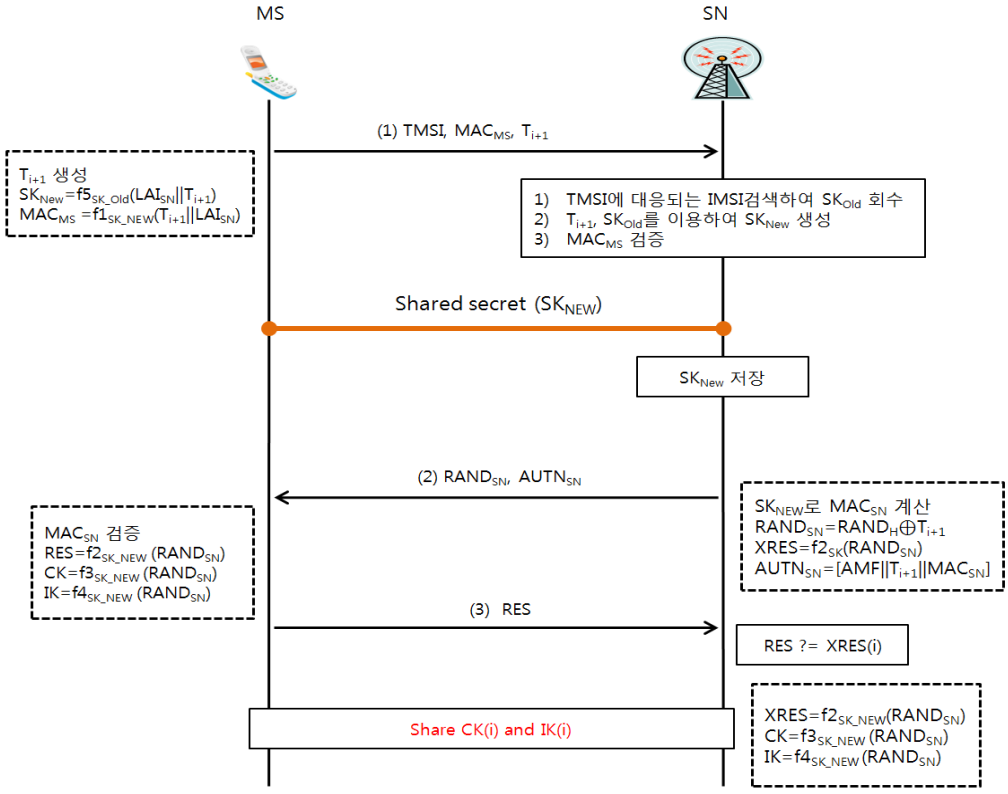
초기 인증과정 완료 후에 인증 벡터가 분배된 후 단말에 대한 재인증이 요구되는 경우의 인증 절차는 그림 3와 같다. 제안하는 재인증 절차는 세션키 갱신을 위해 타임스탬프를 이용하여 HLR과의 통신 없이 세션키를 공유함으로써 SN과 HLR 사이의 시그널링 오버헤드 문제를 효율적으로 개선하였다.

재인증 프로토콜의 시작은 단말이 타임스탬프를 생성하여 $SK_{NEW} = f5_{SK_Old}(LAI_{SN}||T_{i+1})$와 같이 새로운 세션키를 계산하여, 단말의 임시 가입 식별자 TMSI와 MAC_{MS}, T_{i+1}를 사용자 등록 메시지로 SN에 전달한다. SN은 TMSI에 대응되는 IMSI를 찾아 사용자를 식별하고 이전에 사용했던 세션키 SK를 회수하여 단말로부터 전달받은 타임스탬프를 이용하여 새로운 세션키를 계산한다. 이후 MAC_{MS}를 검증하여 단말에 대한 인증과 새로운 세션키 SK_{NEW}에 대한 무결성을 보장할 수 있다. MAC_{MS}에 대한 인증이 성공적으로 이루어지면 새로운 SN_{NEW}는 $RAND_{SN}=RAND_H \oplus T_{i+1}$을 생성하여 MAC_{SN}을 계산하여 단말에게 $RAND_{SN}$과 MAC_{SN}을 전달한다.

(3) 단말의 핸드오버 시 인증 과정

단말의 이동으로 인한 핸드오버가 발생한 경우, 단말과 새로운 SN은 세션키를 공유해야 한다. 제안하는 인증 기법에서는 인증 파라미터 전달 방식을 사용하여 HLR과의 통신 없이 세션키를 공유함으로써 핸드오버로 인한 SN과 HLR 사이의 시그널링 오버헤드 문제를 해결하고 빠른 핸드오버를 지원할 수 있다.

단말의 핸드오버 시에 인증 절차는 단말이 새로운 SN으로 이동을 감지하면 단말은 타임스탬프를 생성하여 새로운 세션 키 $SK_{New}=f5_K(LAI_{SN_NEW}||T_{i+1})$를 계산한 후, 서비스 등록을 위해 사용자 등록 메시지로 TMSI, LAI_{Old},



[그림 3] 제안하는 PE-AKA 재인증 절차

MAC_{MS}, T_{i+1}, KTM(Key Transfer Material)을 전송한다. 여기서 KTM은 단말과 SN 사이에 세션키를 공유하기 위해 무선 구간에서 전송되는 세션키 공유를 위한 파라미터로 다음과 같이 생성된다.

$$KTM=(CK_{Old}\oplus IK_{Old}\oplus SK_{NEW})$$

이후 SN_{New}는 이전 SN의 위치 식별자를 통해 SN_{Old}를 찾아 TMSI, MAC_{MS}, T_{i+1}를 보낸다. SN_{Old}는 TMSI를 통해 단말의 IMSI를 찾아 단말을 식별하고 이전에 사용했던 세션키를 통해 MAC_{MS}를 검증한다.

검증이 성공적으로 이루어지면 마지막에 사용했던 CK와 IK 그리고 인증벡터와 IMSI를 SN_{New}에게 전달한다. SN_{New}는 타임스탬프와 전달받은 $RAND_H$를 이용하여 $RAND_{SN}=RAND_H\oplus T_{i+1}$를 생성하고 새로운 SN_{New}를 인증하기 위한 MAC_{SN}을 생성하여 단말에게 $RAND_{SN}$, MAC_{SN}을 보낸다. 단말은 MAC_{SN}을 검증하여 검증이 성공적으로 이루어지면 새로운 SN_{New}를 인증하고 CK와 IK를 생성하여 비밀통신을 수행한다.

4. 제안 기법의 안전성 및 성능 비교 분석

본 장에서는 제안한 인증 기법에 대한 안전성을 분석하고 관련 연구들과의 성능을 비교 분석한다.

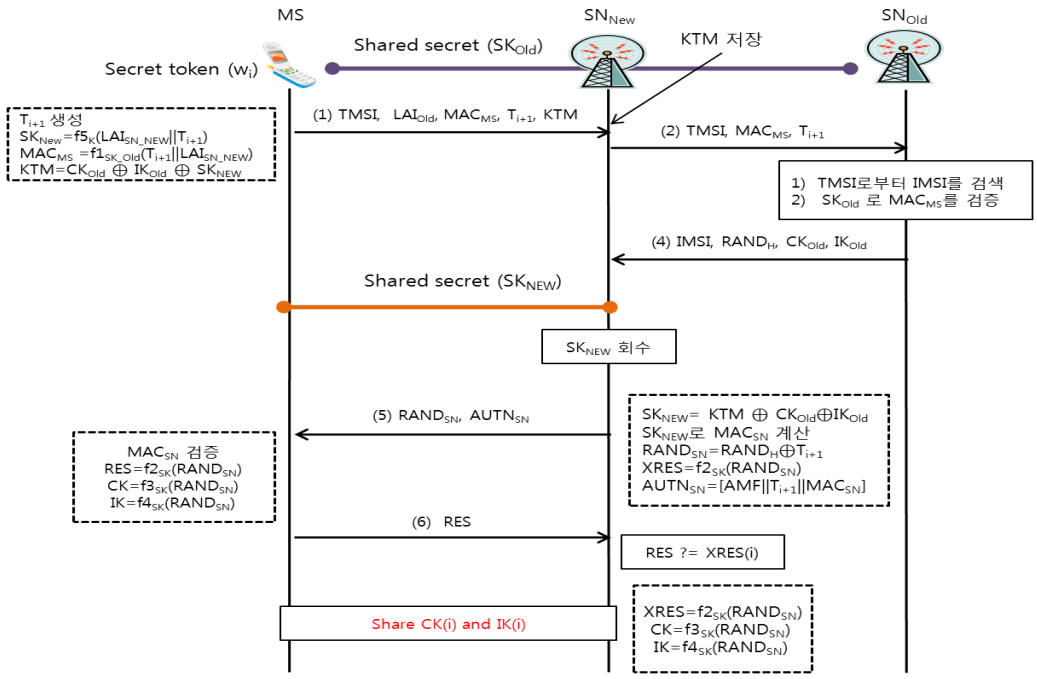
4.1 안전성 분석

- **SQN 동기화 문제**

3GPP-AKA 인증 방식에서 SQN 비동기로 인한 인증 실패 문제가 발생할 수 있다. 제안하는 인증 기법에서는 타임스탬프를 이용하여 유효시간에 전송된 메시지만을 인증함으로써 재전송 공격을 방어하며 동시에 SQN 동기화 문제를 제거하였다.

- **False base station에 의한 공격**

3GPP-AKA 프로토콜은 false base station에 의한 대표적 예인 Redirection Attack에 대해 취약하다. 이는 기존 3GPP-AKA 인증에서 SN은 단순한 메시지 전달자로써 단말은 전달받은 메시지만 인증할 뿐 단말과 SN간의 상



[그림 4] 제안하는 PE-AKA의 핸드오버시 인증 절차

호인증이 완벽히 이루어지지 않기 때문이다. 제안하는 기법에서는 전달되는 메시지 인증 코드 MACMS, MACSN, MACH에 SN의 위치 식별자인 LAISN이 포함되기 때문에 메시지 인증 코드 검증 과정에서 단말이 의도한 SN에 존재하는지를 확인할 수 있다. 따라서 제안하는 인증 기법에서는 단말의 통신 연결이 공격자에 의해 redirect 되는지를 탐지할 수 있으므로, redirection Attack에 대해 안전하다.

- **IMSI 노출에 의한 프라이버시 문제**

제안하는 인증 기법에서는 IMSI의 평문전송이 요구될 경우, 비밀토큰을 이용하여 IMSI를 마스킹하여 전달함으로써 IMSI 평문 전송에 의한 프라이버시 문제를 해결할 수 있다.

- **SN과 HLR 사이의 대역폭 소비 문제**

제안하는 프로토콜에서는 기존 3GPP-AKA 인증에서 사용하는 다수의 인증벡터를 사용하지 않고, 단말을 통해 생성되는 세션키 SK와 하나의 인증벡터를 통해 AKA 절차를 수행함으로써 SN과 HLR 사이의 대역폭 소비 문제를 효율적으로 개선하였다.

- **SN과 HLR 사이의 시그널링 오버헤드 문제**

Juang 등은 임시 키 메커니즘을 사용하여 다수의 인증벡터를 사용하지 않고 임시 키를 통해 단말과 SN간에 AKA 절차를 수행하는 방식을 제안하였다. 그러나 정보통신 환경에서 장시간 하나의 키를 사용하는 것은 안전하지 못하다. 때문에 Juang 등이 제안한 인증 기법에서 임시 키를 갱신하려면 HLR과의 통신이 필수적으로 요구됨으로써 단말이 매번 인증할 때마다 HLR과 통신해야하는 시그널링 오버헤드 문제가 발생할 수 있다. 제안하는 기법에서는 재인증 과정에서 HLR을 경유하지 않고 SN에 저장된 하나의 인증벡터를 이용하여 세션키를 갱신하기 때문에 시그널링 오버헤드 문제를 해결하였다.

- **단말과 SN 사이의 상호인증 향상**

제안하는 인증 기법에서는 상호인증 향상을 위해 MACMS 와 MACSN을 사용한다. 올바른 MAC 값은 정당한 키를 소유한 주체만이 생성할 수 있으므로 전달받은 MAC 값을 검증함으로써 상호인증을 만족할 수 있다.

4.2 관련 연구들과의 성능 비교·분석

본 절에서는 기존 관련 연구들과 제안하는 인증 기법을 비교하여 기술한다. 비교 항목으로는 SN에 대한 인증 데이터 메모리, SN과 HLR 간의 시그널링 오버헤드, SN과 HLR 간의 대역폭 소비 등이다.

[표 2] 제안하는 기법과 관련 연구와의 비교·분석 결과

	3GPP-AKA	Juang등의 인증 기법	Kim등의 인증 기법	제안 기법
SP	No	Yes	Yes	Yes
RA	No	Yes	Yes	Yes
PP	No	Yes	No	Yes
MA	Yes	Yes	Yes	Yes
BC (DS)	No ($688\times N^{*}\times R^{*}$ bit)	Yes ($320\times R^{*}$ bit)	Yes ($468\times R^{*}$ bit)	Yes ($676\times R^{*}$ bit)
SO	Yes	No	No	Yes
인증데이터 크기	RAND : 128 bit, RES : 128 bit, CK : 128 bin, IK : 128 bit, SQN : 48 bit, AK : 48 bit, AMF : 16 bit, MAC : 64 bit, SK : 128 bit, T : 148 bit			

SA: SQN 동기화 문제 해결, RA: Redirection 공격 방어, PP: 프라이버시 문제 해결
MA: 단말과 SN 사이의 상호인증 제공, BC: SN과 HLR 사이의 대역폭 소비 감소
DS: HLR에서 SN으로 전송하는 인증데이터 용량, SO: SN과 HLR 사이의 시그널링 오버헤드 문제 해결
N^{*}: 인증벡터 수, R^{*}: 단말 수

먼저 인증 데이터의 메모리 측면에서 제안하는 기법은 기존의 3GPP-AKA 인증 방식보다 개선된 효과를 보인다. 단말, SN, HLR은 네트워크 접속 인증을 수행하여 상호 인증 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 공간이 필요하다. 제안하는 인증 방식에서는 하나의 인증 벡터만을 사용하여 메모리 저장 측면에서 효율성을 높였다. 그러나 SN은 하나의 인증벡터를 이용하여 인증을 수행하기 위한 계산적인 비용이 증가할 수 있다.

다음으로 SN과 HLR 간의 시그널링 오버헤드 측면에서 제안하는 인증 기법은 초기 인증 과정 후에 일어나는 재인증 과정이나 핸드오버시 인증 과정은 모두 HLR과의 통신 연결 없이 SN과 단말 사이의 공유된 세션키를 통해 인증 절차를 수행할 수 있다. 그러나 Juang과 Kim 등이 제안한 인증 기법에서는 인증을 위한 세션 키 및 임시 키를 갱신하기 위해서는 HLR과의 통신이 요구되기 때문에 잦은 핸드오버로 인한 인증 시 인증 지연이나 시그널링 오버헤드가 발생할 수 있다. 그러나 제안하는 인증 기법은 세션 키를 갱신할 때에도 SCT(Security Context Transfer) 방식을 이용하여 빠른 인증을 수행할 수 있기 때문에 시그널링 오버헤드 측면에서 향상된 성능을 보인다.

마지막으로 인증벡터 분배에 따른 SN과 HLR 사이의 대역폭 소비 측면에서는 기존 3GPP 인증 기법에서는 인증벡터의 수 증가에 따라 SN과 HLR 사이의 대역폭 소비의 부담이 커지나 제안하는 인증 기법은 하나의 인증벡터만을 할당하기 때문에 SN과 HLR 사이의 대역폭 소비를 효율적으로 감소할 수 있다. 그러나 하나의 인증벡터를 장시간 사용할 경우 보안상 취약해 질 수 있다. 따라서 서비스 제공자는 정책적으로 인증벡터의 적절한 교체 주기를 고려해야 한다.

5. 결론

3GPP 이동통신 네트워크는 넓은 사용자 영역과 글로벌 로밍을 지원하는 무선망으로 널리 사용되고 있다. 그러나 무선 구간에서 매체 특성으로 인해 불법적인 변조 및 도청 등 다양한 취약점들이 존재한다. 안전한 서비스를 사용하기 위해 AKA 절차가 필수적이다. 그러나 기존은 3GPP-AKA 방식은 안전한 통신과 빠른 인증 관리를 제공하는데 어려움이 존재한다. 따라서 3G 네트워크 환경에 적용할 수 있는 개선된 인증 메커니즘의 개발이 필요하다.

본 논문에서는 3G 네트워크에서 일어날 수 있는 다양한 취약점을 분석하고, 기존에 제안된 여러 인증 기법들의 특징들을 분석하여 보다 개선된 PE-AKA 프로토콜을 제안하였다. 제안하는 인증 기법에서는 타임스탬프를 이용하여 SQN 동기화 문제와 재전송 공격에 대한 취약점을 제거하였으며, 단말의 영구 가입 식별자인 IMSI 평문 전송으로 인한 프라이버시 침해 문제를 해결하기 위해 비밀토큰 메커니즘을 사용하여 프라이버시 보호를 강화하였다. 그리고 하나의 인증벡터의 사용함으로써 인증 데이터 메모리 저장 오버헤드를 개선하고, 단말의 이동에

따른 핸드오버 시 인증에 대하여 인증벡터를 전달하여 단말의 핸드오버에 따른 인증을 효율적으로 처리할 수 있다는 장점이 있다. 제안하는 인증 프로토콜은 안전하고 효율적인 3G 네트워크를 구축하는 데 활용할 수 있을 것으로 기대한다.

참고문헌

[1] 3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; 3G Security; Security architecture(Release 8)," 3GPP TS 33.102 V8.1.0(2008-12)

[2] 3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; 3G Security; Formal Analysis of the 3G Authentication Protocol(Release 4)," 3GPP TR 33.902 V4.0.0(2001-09)

[3] 3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms (Release 1999)," 3GPP TR 33.909 V1.0.0(2000-12)

[4] 3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set; An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2,f3,f4,f5 and f5*; Document 1: generan(Release 8)," 3GPP TS 35.205 v8.0.0(2008-12)

[5] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Transactions on Wireless Communication, Vol. 4, no. 2, pp. 734-742 Mar. 2005.

[6] Chris J.Mitchell, "The Security of the GSM air interface protocol", Univ. of London, Royal Holloway, Technical Report, RHUL-MA-2001244-250, Nov. 1993.

[7] 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.

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

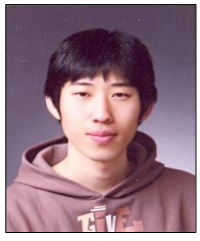
[9] 이옥연, “무선통신 보안”, 물리학과 첨단기술 제16권 3호, pp. 22-26, 2007. 3.

[10] 박정현, 임선배, 이경준, “이동통신 보호를 위한 인증 방식 분석”, 전자통신동향분석 제13권4호, pp1-20, 1998. 8.

[11] 김두환, 정수환, “3GPP 네트워크에서 효율적인 인증 데이터 관리를 위한 개선된 AKA 프로토콜”, 정보보호학회 논문지 제19권2호, pp. 93-103, 2009. 4.

[12] 김대영, 최용강, 김상진, 오희국, “프라이버시와 완전한 전방향 안전성을 제공하는 UMTS 키 동의 프로토콜”, 정보보호학회논문지 제17권 3호, pp81-90., 2007. 6.

전 서 관(Seo-Kwan Jeon) **[정회원]**



- 2008년 2월 : 호서대학교 정보보호학과(공학사)
- 2010년 2월 : 호서대학교 정보보호학과(공학석사)
- 2010년 3월 ~ 현재 : 한국시스템보증(주) 연구원

<관심분야>
네트워크 보안, 정보보호 평가 및 인증

오 수 현(Soo-Hyun Oh) **[정회원]**

- 1998년 2월 : 성균관대학교 정보공학과(공학사)
- 2000년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부(공학석사)
- 2003년 8월 : 성균관대학교 전기전자 및 컴퓨터공학부(공학박사)
- 2004년 3월 ~ 현재 : 호서대학교 정보보호학과 교수

<관심분야>
정보보호론, 네트워크 보안, 정보보호 평가 및 인증