3G-WLAN 상호연동: EAP-AKA에 기반을 둔 새로운 인증 및 키 합의 프로토콜

문혜란, 한규석, 김광조*

*한국정보통신대학교(ICU), 국제정보보호기술연구소

3G-WLAN Interworking: New Authentication and Key Agreement Protocol based on EAP-AKA

Hyeran Mun, Kyusuk Han, Kwangjo Kim*

* International Research Center for Information Security (IRIS),

Information and Communications University (ICU), Korea

요 약

3rd Generation Partnership Project(3GPP) 표준은 차세대 모바일 통신 시스템을 위해 SAE (System Architecture Evolution)/ LTE (Long Term Evolution)을 개발하고 있으며 이 SAE/LTE 구조는 안전하게 서비스를 제공하면서 3G-WLAN의 상호연동을 지원하고 있다 [1]. 3G 환경은 효율적인 과금(Charging)관리, 로밍관리 그리고 넓은 서비스 범위를 제공하며 WLAN은 높은 대역폭, 높은 전송률 그리고 인터넷과의 호환성 등을 제공하지만 3G 환경에 비해 비교적 좁은 서비스 범위를 제공한다. 따라서 3G-WLAN을 상호연동을 하면 3G, WLAN이 가지고 있는 이점을 모두 가질 수 있기 때문에 3G-WLAN의 상호연동을 위한 연구가 활발히 이루어지고 있다. 상호 연동 시, 안전한 통신을 위해서는 두 네트워크간의 상호 인증 및 데이터 암호화 등이 요구되기 때문에 여러 인증 및 키 합의 프로토콜이 제안되고 있다. 하지만 이러한 프로토콜은 여전히 취약점을 가지고 있다. 따라서 본 논문은 EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement) 프로토콜을 기반으로 한 새로운 인증 및 키 합의 프로토콜을 제안한다. 제안한 프로토콜을 통하여 보다 안전하고 효율적으로 3G-WLAN의 상호연동을 할 수 있다.

I. 서론

차세대 모바일 통신 시스템은 더 안전하고 빠른 통신을 위해 발전하고 있다. 3rd Generation Partnership Project(3GPP) 그룹에서 개발 중인 SAE (System Architecture)/ LTE (Long Term Evolution) 구조는 3GPP TS 33.102 [2]에서 기술되고 있는 보안구조에 비해 더 안전한 통신을 제공한다. 그림 1은 SAE/LTE의 전체 구조를 간단히 보여주고 있다 [3]. 그림 1과 같이 SAE/LTE 구조는 3가지 타입에 접근 할 수 있으며 각각의 타입에 안전하게 접근하기 위해 여러 인증 및 키 합의 프로토콜을 제시하고 있다 [4], [5]. WLAN과 같은 Non-3GPP 환경에 접근하기 위해서는 [6]에서 제시된 EAP-AKA을 재사용하며 E-UTRAN을 통해 단말기와 MME(Mobility Management Entity) 간의 인증 및 키 합의 프로토콜은 [2]에서 제시된 UMTS-AKA을 재사용한다. EPS(Evolved Packet System)-AKA라 불리는 이 인증 및 키 합의 프로토콜을 수행하면 그림 2와 같이 중간 키 K_{ASME}을 생성하게 된다 [4]. K_{ASME}을 이용하면 5개의 키를 생성할 수 있는데 생성된 키들은 단말기와 MME, 단말기와 eNodeB, 단말기와 Serving GW 간의 통신에서

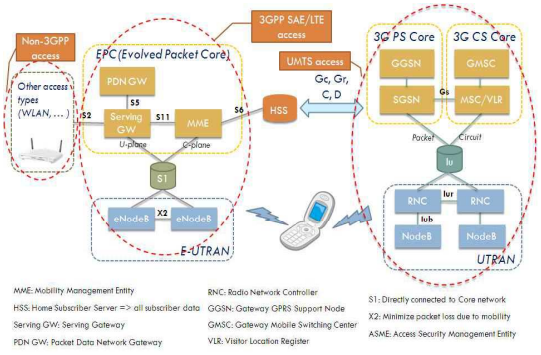
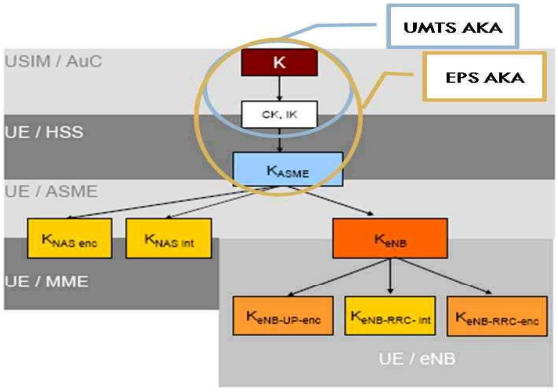


그림 1. SAE/LTE 전체 구조

의 무결성과 기밀성 보호를 위해 사용된다. 3G-WLAN의 상호연동을 지원하기 위해서 대표적으로 EAP-AKA[6], EAP-SIM[7]가 존재하며 EAP-AKA는 [2]에서 제시된 UMTS-AKA(Universal Mobile Telecommunication System-Authentication and Key Agreement)에 기반하고 있다. 모바일 가입자가 WLAN에 접근을 시도할 때 모바일 가입자는 AP (Access Point)에 접근하여 NAI(Netwoek Access Identifier)을 통해 사용자 식별 정보가 포함되어 있는 IMSI(International Mobile Subscriber Identity)을 제공하며 이 IMSI는 USIM에 저장되어 있다. 하지만 EAP-AKA은 UMTS-AKA을 기반으로 하고 있기 때문에 UMTS-AKA가 가지고 있는 취약성뿐만 3G-WLAN 상호 연동 시 발생 할 수 있는 취약점도 가지고 있다. 따라서 본 논문에서는 EAP-AKA 프로토콜을 기반으로 한 새로운 인증 및 키 합의 프로토콜을 제안한다. 제안하는 프로토콜은 UMTS-AKA에서 나타나는 SQN(Sequence Number) 동기화 등의 문제를 해결하며 IMSI 노출 등으로 일어나는 사용자 프라이버시 침해를 해결하고 더 강화된 안정성을 보장하기 위해 완전 순방향 비밀성(Perfect Forward Secrecy: PFS)를 제공한다. 또한 재전송 공격(Replay attack), 중재자 공격(Man-in-the-middle attack)을 막을 수 있다.



KNASint: Protection of NAS traffic with particular integrity
KNASenc: Protection of NAS traffic with particular encryption
KUPenc: Protection of UP traffic with particular encryption
KRRCint: Protection of UP traffic with particular integrity
KRRCenc Protection of NAS traffic with particular encryption.

그림 2. 키 계층구조

본 논문의 나머지 구성은 다음과 같다. 2장에서는 3G-Non 3G 상호연동 구조와 EAP-AKA에 대해 간단히 살펴본다. 3장에서는 EAP-AKA 프로토콜을 기반으로 한 새로운 인증 및 키 합의 프로토콜을 제안한다. 4장에서는 제안한 프로토콜을 기존 방식과 비교를 하며 5장에서는 본 논문의 결론을 제시한다.

II. 관련연구

2.1 3G-Non 3G 상호연동 구조

그림 3은 SAE/LTE 구조가 Non-3GPP 환경에 접근하는 구조를 보여준다. 그림 3에서 보듯이 Non-3GPP 환경에는 WiMAX와 같은 신뢰된 Non-3GPP로의 접근과 WLAN과 같은 신뢰되지 않은 Non-3GPP로의 접근으로 구성된다.

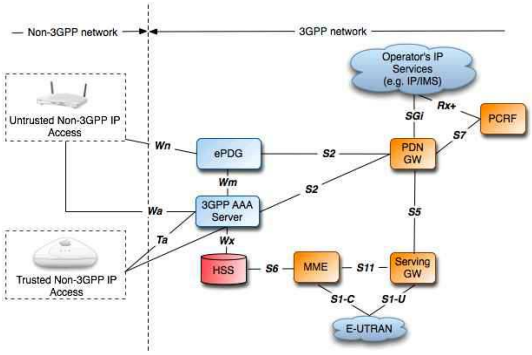


그림 3. 3G-Non 3G network 상호연동

AAA(Authentication, Authorization and Accounting) 서버는 3G환경과 Non-3GPP 환경과의 안전한 접근을 위해 단말기와 상호 인증을 수행하며 Wx 인터페이스를 통해 HSS(Home Subscriber Server)에 접근하여 IMSI와 같은 사용자 정보와 인증벡터를 얻어내는 등 3G-Non 3G 환경의 상호연동 시 중요한 역할을 수행한다. Ta 인터페이스는 신뢰된 Non-3GPP와 연결되어 있어 인증, 권한, 과금과 관련된 정보를 안전한 방법으로 전송하는 역할을 한다. 또한 S2 인터페이스를 통해 사용자 데이터는 신뢰된 Non-3GPP IP access network로부터 PDN GW로 전송된다.

WLAN와 같은 신뢰되지 않은 Non-3GPP IP access network에 접근하기 위해서는 ePDU개체가 더 추가된다. ePDU(evoloved Packet Data Gateway)는 신뢰되지 않은 Non-3GPP에서 발생되는 모든 트래픽들이 집중되는 곳이며 IPSec을 이용해 안전한 터널을 구축하여 사용자 데이터를 안전하게 전송하는 역할을 한다. 또 Wm인터페이스는 AAA서버에서 ePDU로 사용자와 관련된 정보를 보내는 역할을 한다.

2.2 EAP-AKA 과정

EAP-AKA는 UMTS-AKA에 기반하고 있으며 UE(User Equipment)와 AAA 서버 사이의 상호 인증을 제공한다. EAP-AKA는 UMTS-AKA을 재사용하여 암호화키(*CK*: Cipher Key), 무결성 키(*IK*: Integrity Key)를 생성하며 이를 이용해 EAP-Master Key(*MK*)를 생성한 후 이를 이용해 Master Session Key(*MSK*)를 생성한다. 생성된 *MSK*는 AP에 EAP Success 메시지와 함께 전달되어서 다음 통신 과정을 보호하는데 사용된다. 그림 4은 EAP-AKA의 전체 과정을 보여주고 있다. 과정 6~9 에서 보듯이 AAA 서버는 사용자 식별정보를 다시 한 번 요청하게 되는데 이는 중간에 다른 개체가 EAP Response/Identity 메시지에 포함된 IMSI 같은 사용자 식별 정보를 변화시키거나 대체시킬 수 있기 때문이다. 따라서 UE는 EAP Request/AKA-Identity 메시지를 받으면 EAP Response/Identity 메시지에 포함된 IMSI 와 같은 사용자 식별정보를 AAA 서버에게 보낸다. 따라서 AAA 서버는 이 과정에서 받은 사용자 식별 정보를 기반으로 남은 인증 및 키 합의 과정을 수행하게 된다. 과정 10에서 보듯이 AAA 서버는 WLAN 접근 프로파일을 체크하여 적당

한 권한을 가진 사용자가 WLAN서비스를 사용하는지 검

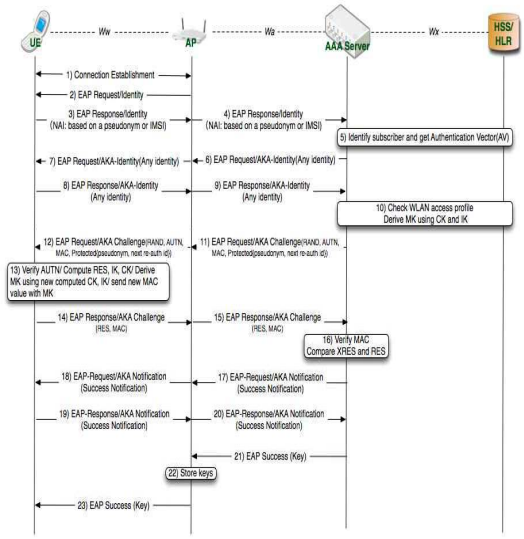


그림 4. EAP-AKA 전체 과정

증한다. 그림 5는 UE와 AAA 서버 사이에서 생성되는 MK와 MSK의 생성 절차를 보여준다.

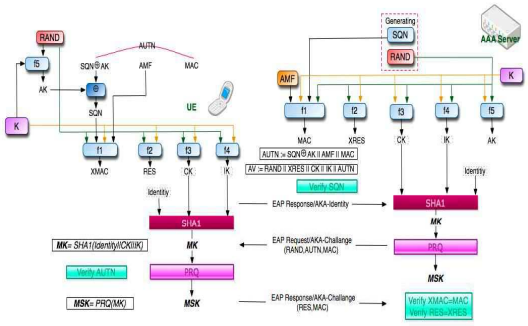


그림 5. MK, MSK 키 생성 절차

2.3 EAP-AKA 취약점

EAP-AKA가 가지고 있는 취약점은 다음과 같다.

- IMSI 노출: 임시 사용자 식별 정보를 생성하여 사용한다고 하더라도 처음 EAP-AKA를 수행할 때에는 IMSI가 AAA 서버에 보내져야 한다. 만약 IMSI의 정보를 공격자가 얻게 된다면 사용자 추적 등 악의적인 목적으로 사용 될 수 있다.
- 중재자 공격(Man-in-the middle attack): IMSI가 적어도 한번은 평문으로 AAA 서버에게 전송되기 때문에 공격자는 IMSI가 전송되는 것을 기다렸다가 IMSI를 얻어 수정할 수 있다. 그리고 UE와 AAA서버 사이에 인증이 성공하더라도 EAP Success 메시지가 아무런 암호화 작업 없이 MSK와 함께 AP와 단말기에 전송되기 때문에 공격자는 AP로 위장하여 메시지를 수신하고 이 메시지를 수정하여 단말기에 전송시킬 수 있다.
- 완전 순방향 비밀성(Perfect Forward Secrecy: PFS): EAP-AKA는 UMTS-AKA와 같이 UE와 HSS 사이에서 공유하고 있는 대칭키 K를 기반으로 인증 및 키 합의 과정이 수행된다. 따라서 K가 노출되는 것은 인증 및 키 합의 과정이 노출되는 것과 같다. 즉, EAP-AKA는 완전 순방향 비밀성이 제공되지 않는다.
- SQN 동기화 문제: EAP-AKA는 UMTS-AKA에서 사용하는 AV(Authentication Vector)를 사용하고 있기 때문에 UE는 AAA로부터 받은 시퀀스 넘버 SQN의 범위가 올바르지 않으면 UE는 SQN 동기화를 실행한다. SQN동기화 과정과 함께 AAA 서버가 HSS에게 한 번 더 AV를 요구해야 하기 때문에 AAA서버와 HSS 사이의 대역폭 소비가 일어나 성능 면에서 매우 비효율적이다.

III. 제안방식

3.1 기호 표시 및 가정

제안하는 방식은 다음과 같은 기호와 가정을 가진다.

- UE(User Equipment)는 현재 접근 할 수 있는 AAA 서버와 AN(Access Network)의 ID를 식별할 수 있다.
- AAA 서버와 HSS사이는 보안채널(Secure channel)로 설립되어 있다.

표 1.기호 표시 및 설명

기호	설명
${}_cID_{UE}$	UE(User Equipment)의 현재 임시 ID
${}_pID_{UE}$	UE(User Equipment)의 이전 임시 ID
T_x	개체 x가 생성하는 타임스탬프
ID_x	개체 X의 ID
g_k^i	키 k를 이용한 키 생성 함수(i값에 따라 다른 키 생성)
f_k^1, f_k^2	f_k^1 : 키 k를 이용해 MAC생성, f_k^2 : ${}_cID_{UE}$ 생성
$RAND_x$	개체 x가 생성하는 랜덤 넘버
K_{xy}	개체 x와 y사이에서 공유한 대칭키
U, H	각각 UE와 HSS을 나타냄

3.2 제안하는 프로토콜 설명

그림 6는 제안하는 프로토콜의 전체 과정을 보여주고 있다.

- 과정 1: UE와 AP사이에 접속 설정을 한다.
- 과정 2: AP(Access Point)는 UE에게 EAP Request/Identity 메시지를 보내 사용자의 식별 정보를 요청한다.
- 과정 3: UE는 EAP Request/Identity에 대한 응답으로 T_U을 생성하고 UE와 HSS가 미리 공유한 대칭키 K_{UH}을 이용하여 $MAC_U = f^1_{K_{UH}}(T_U \| ID_{AAA} \| ID_{AP})$을 생성한다. 또 IMSI의 노출을 막기 위해 UE와 HSS가 공유한 대칭키 K_{UH}을 이용하여 ${}_cID_{UE} = f^2_{K_{UH}}(IMSI)$ or $f^2_{K_{UH}}({}_pID_{UE})$을 계산한다. 이

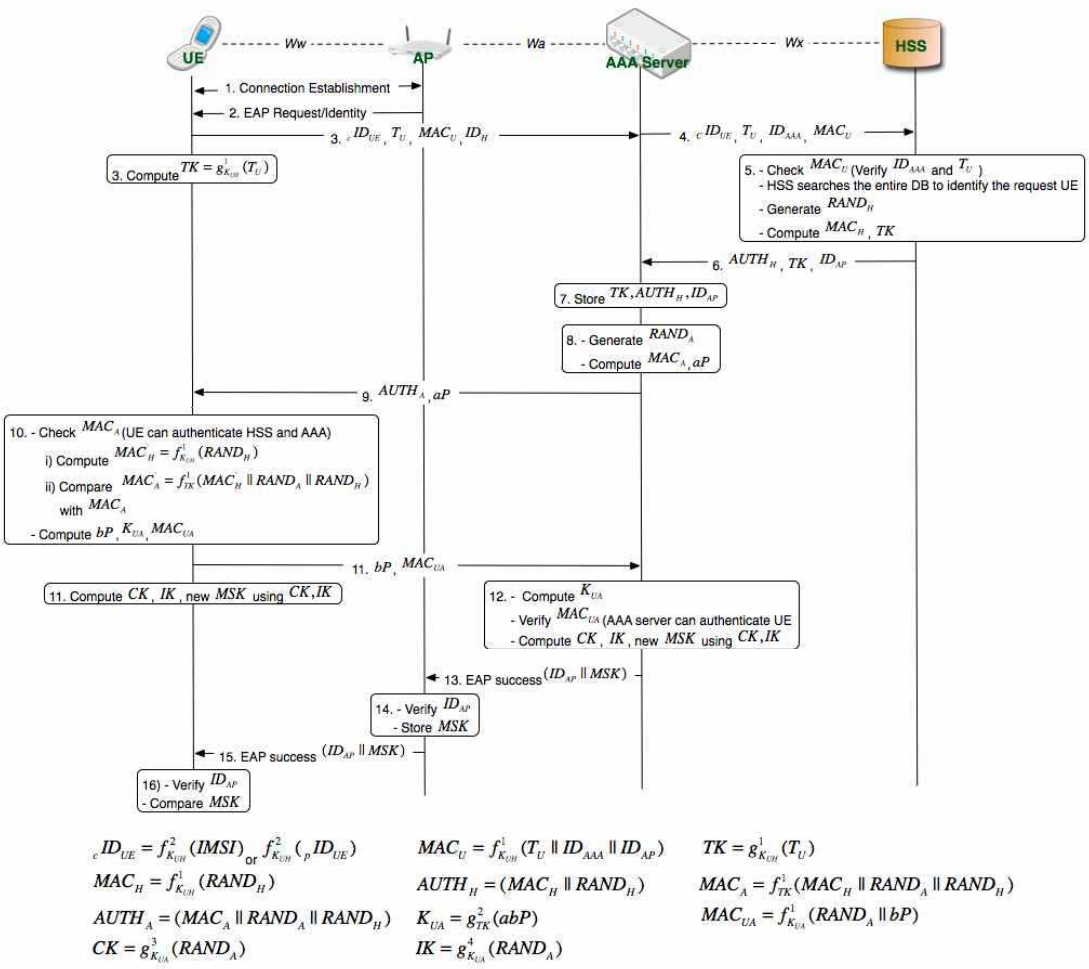


그림 6. 제안하는 프로토콜 전체과정

로 인해 사용자 프라이버시 침해를 막을 수 있으며 중재자 공격도 막을 수 있다. UE는 AP에게 $_cID_{UE}, T_U, MAC_U, ID_H$을 보내고 동시에 자신이 생성한 타임 스탬프 T_U와 UE와 HSS가 미리 공유한 대칭키 K_{UH}을 이용해 TK을 계산한다.

- 과정 4: AAA 서버는 $_cID_{UE}, T_U, ID_{AAA}, MAC_U$을 과정 3에서 받은 ID_H를 이용해 HSS에 전달한다.
- 과정 5: HSS은 과정 4에서 받은 MAC_U을 검증한다. HSS는 MAC_U을 통해 ID_{AAA}, ID_{AP}, T_U을 유추하고 $MAC_U = f^1_{K_{UH}}(T_U \| ID_{AAA} \| ID_{AP})$을 통해 얻은 ID_{AAA}와 메시지를 보낸 AAA 서버가 같은지 확인한다. 그 다음 받은 T_U가 적절한 범위에 있는지 확인한 후 받은 T_U와 MAC_U을 통해 얻은 T_U가 같은지 확인하여 UE을 인증한다. 이 과정은 재전송 공격(Replay attack)을 막을 수 있으며 T_U을 이용해 임시키 $TK = g^1_{K_{UH}}(T_U)$을 생성한다. HSS은 IMSI, 현재 그리고 이전 임시 ID가 저장된 전체 DB을 검색함으로써 요청한 UE을 식별한다. 또 HSS은 $RAND_H$을 생성하며 이를 이용해 $MAC_H = f^1_{K_{UH}}(RAND_H)$을 생성한다.
- 과정 6: HSS은 AAA 서버로 $AUTH_H = (MAC_H \| RNAD_H), TK, ID_{AP}$을 전달한다.
- 과정 7: AAA 서버는 과정 6에서 받은 TK, $AUTH_H$, ID_{AP}을 저장한다.
- 과정 8: AAA 서버는 $RAND_A$을 생성한 후 $MAC_A = f^1_{TK}(MAC_H \| RAND_A \| RAND_H)$을 계산한다. 그 다음 임의의 수 a을 선택하여 타원곡선에서 aP을 계산한다.

(타원곡선 Diffie-Hellman: 사용자 A와 B는 우선 자기 자신의 개인키와 공개키를 만들기 위해 유한체 F와 그 위에 정의되는 타원곡선 E을 결정해 공개하고 위 수가 충분히 큰 E의 원소 P도 선택하여 공개한다. 사용자 A와 B는 각각 E에서의 임의의 수 a,b을 선택하

여 자신의 개인키로 보관하고 aP,bP을 각각 계산하여 공개한다. 그 다음 각각 자신의 개인키와 공개된 키를 이용해 둘 사이의 비밀키 abP을 구한다. [10])

- 과정 9: AAA 서버는 UE에게 $AUTH_A = (MAC_A \| RAND_A \| RNAD_H), aP$을 보낸다.
- 과정 10: UE는 MAC_A을 검증하여 HSS와 AAA 서버를 인증할 수 있다. MAC_A을 검증하는 순서는 다음과 같다.

  a) $MAC_H^{'} = f_{K_{UH}}^1(RAND_H)$을 계산한다.

  b) $MAC_A^{'} = f_{TK}^1(MAC_H^{'} \| RAND_A \| RAND_H)$가 받은 MAC_A와 같은지 확인한다.

  UE는 $MAC_A^{'}$을 통해 MAC_H가 HSS로부터 생성된 것인지 확실히 확신 할 수 있으며 이는 재전송 공격과 중재자 공격을 막을 수 있다. 그 후 UE는 임의의 수 b을 선택해 타원곡선에서 bP을 계산하고 과정 9에서 받은 aP을 이용해 AAA 서버와 UE 사이의 대칭키 $K_{UA} = g_{TK}^2(abP)$을 생성한다. 생성된 K_{UA}을 이용해 $MAC_{UA} = f_{K_{UA}}^1(RAND_A \| bP)$을 계산한다.
- 과정 11: UE는 bP, MAC_{UA}을 AAA 서버에 보내는 동시에 CK,IK을 각각 계산한다. 생성한 암호화키와 무결성 키를 이용하여 EAP-AKA와 같이 $MSK(MasterSessionKey)$을 생성한다.
- 과정 12: AAA 서버는 UE로부터 받은 bP을 이용해 대칭키 K_{UA}을 계산한다. 그 후 MAC_{UA}에 포함된 $RAND_A$과 과정 8에 생성한 $RAND_A$이 같은 지 확인한다. 따라서 AAA서버는 MAC_{UA}을 검증하고 UE는 과정 10에서 MAC_A을 검증함으로써 AAA 서버와 UE은 서로를 상호 인증 할 수 있다. 검증 후 CK,IK을 계산하고 생성된 키들을 이용하여 EAP-AKA와 같이 MSK을 생성한다.
- 과정 13: AAA 서버는 EAP success 메시지와 함께 과정 6에서 받은 AP의 ID인 ID_{AP}와 과정 12에서 생성한 MSK이용해 $ID_{AP} \| MSK$을 AP에게 보낸다.
- 과정 14: AP는 과정 13에서 받은 ID_{AP}와 자신의 ID와 같은지 확인 후 같으면 MSK을 저장한다.
- 과정 15: AP는 UE에게 EAP success 메시지와 함께 ID_{AP}와 과정 14에서 계산한 MSK을 이용해 $ID_{AP} \| MSK$을 UE에게 보낸다.
- 과정 16: UE는 과정 3에서 MAC_U을 생성할 때 이용한 ID_{AP}와 과정 14에서 받은 ID_{AP}가 같은지 확인하고 과정 11에서 계산한 MSK와 과정 15에서 받은 MSK가 같은지 확인한다. 같으면 성공적인 인증 및 키 합의과정이 이루어 진 것으로 AP와 UE가 가지고 있는 MSK을 이용해 UE는 안전하게 WLAN 서비스를 사용할 수 있다. 이러한 과정으로 제안하는 프로토콜은 EAP-AKA에서 나타날 수 있는 중재자 공격을 막을 수 있다.

IV. 기존 방식과 비교

WLAN을 인증하기 위해 IEEE 802.1x에서는 EAP(Extensible Authentication Protocol)을 기반으로 한 인증 프레임워크를 제공한다. EAP는 여러 개의 인증 프로토콜을 지원하고 있는데 이는 각각 장점과 단점을 가지고 있다. 표 2에서는 제안된 EAP 인증 프로토콜과 본 논문에서 제안한 프로토콜의 비교표를 제시하고 있다 [15]. 제안한 프로토콜은 EAP-AKA와 EAP-SIM과 함께 Cellular-WLAN의 상호 연동을 지원하며 IMSI와 같은 사용자 식별 정보를 보호한다. 하지만 제안한 프로토콜은 EAP-TTLS와 PEAP와 같이 공개키 기반이 아닌 대칭키와 ECDH (Elliptic Curve Diffie-Hellman)을 사용하기 때문에 EAP-TTLS와 PEAP에 비해 오버헤드가 적게 발생한다. 또한 IMSI가 중재자 공격과 재전송 공격을 막고 완전 순방향 비밀성을 제공하며 UMTS-AKA에 기반을 두고 있는 EAP-AKA에서 발생할 수 있는 SQN 동기화 문제가 발생하지 않아 성능 측면에서 더 효율적이다.

V. 결론

본 논문에서는 EAP-AKA 프로토콜을 기반으로 한 새로운 인증 및 키 합의 프로토콜을 제안하고 있다. 제안한 프로토콜은 대칭키 기반 암호 시스템과 ECDH(Elliptic Curve Diffie-Hellman)를 기반으로 하여 3G-WLAN 상호 연동을 지원한다. 또한 중재자 공격, 재전송 공격을 방지할 수 있으며 완전 순방향 비밀성을 제공하고 IMSI와 같은 사용자 식별 정보를 완벽히 보호한다. UMTS-AKA에 기반을 두고 있는 EAP-AKA에서 발생할 수 있는 SQN 동기화 문제가 발생하지 않아 성능 측면에서 더 효율적이다. 따라서 제안한 논문을 통하여 보다 안전하고 효율적으로 3G-WLAN의 상호연동을 할 수 있다.

참고문헌

[1] Third Generation Partnership Project (3GPP) specifications and reports, TR xx.xxx (Technical Report) or TS xx.xxx (Technical Spec.) available at http://www.3gpp.org/ftp/Specs/html

[2] Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v7.1.0 "3G Security; Security Architecture(Release 7)", December 2006

[3] Pierre Lescuyer, Thierry Lucidarme, "Evolved Packet System(EPS): The LTE and SAE Evolution of 3G UMTS", J.Wiley & Sons, 2008

[4] Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.0.0 "3GPP System Architecture Evolution(SAE): Security architecture(Release 8)", June 2008

[5] Third Generation Partnership Project (3GPP), 3GPP TR 33.821 v1.0.0 " Rationale and track of suecirty decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)", December 2007

[6] J. Arkko, H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", IETE RFC 4187,

표 2. 기존 EAP 프로토콜과 제안한 프로토콜의 비교

	제안한 프로토콜	EAP-TLS [11]	EAP-TTLS [12]	PEAP[13]	EAP-AKA[6]	EAP-SIM [7]	EAP-UTLS [14]
암호 메커니즘	대칭키 기반, ECDH	공개키 기반 (인증서 사용)	공개키 기반 (인증서 사용)	공개키 기반 (인증서 사용)	대칭키 기반	대칭키 기반	공개키 기반 (인증서 사용)
구독자 관리 주체	Cellular network 제공자	WLAN 제공자	WLAN 제공자	WLAN 제공자	Cellular network 제공자	Cellular network 제공자	Cellular network 제공자
사용자 식별 정보(IMSI) 보호	O	X	O	O	X	X	O
3G-WLAN 상호연동	O	X	X	X	O	O	O
중재자 공격에 안전	O	O	X	X	X	X	O
재전송 공격 안전	O	O	O	O	O	O	X
완전 순방향 비밀성 제공	O	X	X	X	X	X	X
SQN 동기화	X	-	-	-	O	-	-

January 2006

[7] H. Haverinen, J. Salowey, "EAP SIM Authentication",draft-arkko-pppext-eap-sim-12, IETF, October 2003

[8] Third Generation Partnership Project (3GPP), 3GPP TS 23.402 v8.2..0 "Architecture enhancements for non-3GPP accesses(Release 8) ", June 2008

[9] Third Generation Partnership Project (3GPP), 3GPP TS 33.234 v8.1.0 "3G security: Wireless Local Area Network(WLAN) interworking security(Release 8)", March 2008

[10] 이만영, 원동호 공저, "현대 암호학 및 응용", 생능출판사, 2002

[11] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, RFC 2716, IETF, October 1999

[12] P. Funk, S. Blake-Wilson, EAP Tunneled TLS Authentication Protocol,draft-ietf-pppext-eap-ttls-05, IETF, July 2004

[13] A. Palekar, D. Simon, S. Josefsson, H. Zhou, G. Zorn, Protected EAP Protocol (PEAP) Version 2, draft-josefsson-pppext-eap-tls-eap-10.txt, IETF, October 2004

[14] Yuh-Min Tseng, USIM-based EAP-TLS authentication protocol for wireless local area networks, Computer Standards & Interfaces, November 2007

[15] L. Han, A threat Analysis of the Extensible Authentication Protocol, Honors Project Report, April 2006