논문 2009-46TC-5-22

이질적인 무선 네트워크 환경에서 인증 연동을 위한 비 UICC 방식의 EAP-AKA 인증

(EAP-AKA Authentication without UICC for Interworking Authentication in Heterogeneous Wireless Networks)

최 재 덕*, 정 수 환**

(Jaeduck Choi and Souhwan Jung)

요 약

본 논문에서는 3GPP 시스템 중심의 WLAN/WiBro 네트워크 연동 환경에서 UICC를 사용하지 않는 EAP-AKA 인증을 제안한다. UICC 방식의 EAP-AKA 인증을 기존 WLAN/WiBro 단말들에게 적용하기 위해서는 기존 무선 단말들이 UICC를 추가로 장착해야 하기 때문에 비용 부담이 있고, WLAN/WiBro 이동 단말의 구조적인 문제로 UICC를 장착할 수 없을 경우 인증 연동에 어려움이 있다. 만약 이러한 이유로 이동 단말들이 UICC 장착 없이 EAP-AKA를 사용한다면, UICC에 저장되어 있는 128 비트의 long-term 비밀키가 단말에 저장되기 때문에 비밀정보 저장에 있어서 매체 분리 원칙에 위배되어 안전성이 떨어지고, 이동 단말이 바뀔 경우 long-term 비밀키 이동에 대한 불편함이 발생한다. 제안 기법은 Diffie-Hellman 암호 알고리즘과 사용자 패스워드를 사용하여 UICC 기반의 EAP-AKA와 같은 수준의 안전성과 편리한 이동성 및 휴대성을 제공한다. 또한 기존 3GPP 시스템 인증 구조의 큰 수정을 요구하지 않지 않기 때문에 통합 무선 네트워크에 인증 기법으로 적합하다.

Abstract

This paper proposes the EAP-AKA scheme without UICC for extending its usage to existing WLAN/WiBro devices. To apply the current EAP-AKA scheme, the WLAN/WiBro devices require an external Universal Integrated Circuit Card (UICC) reader. If they don't use UICC due to cost overhead and architectural problem of device, the EAP-AKA scheme loses its own advantages in security and portability aspects. The proposed scheme uses the DH key algorithm and a password for non-UICC devices instead of using the long-term key stored in UICC. The main contribution is to maintain the security and portability of the EAP-AKA while being applied to non-3GPP network devices not equipped with UICC. Furthermore, it does not require major modifications of authentication architecture in 3GPP.

Keywords: EAP-AKA, Non-UICC, 3GPP, WiBro, WLAN

I. 서 론

무선 인터넷을 이용할 수 있는 3GPP, WLAN, WiBro 네트워크에 대해서 3GPP 시스템 중심으로 WLAN과 WiBro 네트워크를 연동하는 연구가 많이 이루어지고 있다[1~5]. 3GPP는 폭 넓은 통신 반경과 글로벌 로밍 기능을 제공하는 장점이 있지만, 데이터 전송율이 낮은 단점이 있다. WLAN은 높은 데이터 전송율을 제공하지만, 핫 스팟 존과 같이 좁은 지역에서만 인터넷 이용이 가능하다. WiBro는 고속 이동 중에도 사용자에게 비교적 높은 데이터 전송율을 제공해주는 무선 네트워크 기술이다. 이와 같이 각 무선 네트워크들의 장단점을 고려하여 네트워크 연동이 이루어진다면

* 정회원, ** 평생회원, 숭실대학교 정보통신전자공학부
(School of Electronic Engineering, Soongsil University)

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 산업원천기술개발사업의 일환으로 수행하였음. [2008-F015-02, 서비스 가용성을 위한 이동성 관리 기술 연구]

접수일자: 2009년12월18일, 수정완료일: 2009년5월18일

무선 인터넷 사용자들은 언제 어디서나 최적의 상태로 인터넷을 이용할 수 있다.

이질적인 네트워크 기술 간 연동에 있어서, 동일한 인증 기술 연구는 과금 서비스 통합, 가입자 관리용이, 끊김 없는 네트워크 액세스 및 핸드오버 등을 지원할 수 있는 기초 기술이기 때문에 중요하다. 현재 3GPP와 WLAN 네트워크의 인증 연동에 대한 연구가 EAP-AKA 인증 방식과[6~10] 비 EAP-AKA 방식으로[11~13] 나누어져 다양하게 연구되고 있지만, 3GPP 시스템 기반으로 WLAN 및 WiBro 네트워크가 연동될 때, 인증 구조 또한 3GPP 시스템의 인증 구조를 사용하는 것이 유리하다. 왜냐하면, 3GPP 네트워크는 이미 많은 가입자를 확보하여 과금, 로밍, 안전한 인증 및 키 교환 방법 등에서 잘 운영되고 있기 때문이다. 또한 이미 폭넓게 설치된 3GPP의 인증 구조에서 EAP-AKA 인증 방식을 사용하는 것은 3GPP, WLAN, WiBro 네트워크 연동 과정에서 추가 설치비용 없이 적용할 수 있는 이점이 있기 때문이다.

그러나 기존 WLAN/WiBro 단말기에서 EAP-AKA를 사용하기 위해서는 UICC (Universal Integrated Circuit Card)를 장착해야 하는 요구사항이 있다[3, 7~9, 14]. 즉 3GPP의 EAP-AKA 인증 방식은 UICC를 사용하기 때문에 기존 WLAN/WiBro 단말들이 EAP-AKA를 사용하기 위해서는 UICC 장착에 따른 추가 비용이 필요하다. 만약 비용 부담 및 UICC 장착에 대한 구조적 어려움 때문에 UICC 사용 없이 WLAN/WiBro 단말기에 128 비트의 long-term 비밀키를 저장하고 EAP-AKA를 사용한다면, long-term 비밀키가 단말에 저장되기 때문에 비밀 정보 저장에 있어서 매체 분리 원칙에 어긋나 안전성이 떨어지고, 단말이 바뀔 경우 long-term 비밀키를 이동시키거나 새로 할당 받아야 하는 불편함이 발생한다. 따라서 비 UICC 방식의 기존 단말들이 EAP-AKA를 사용할 때, UICC 방식의 EAP-AKA와 같은 수준의 안전성 및 휴대의 편리성을 제공할 수 있는 인증 방법이 필요하다.

본 논문에서는 기존 WLAN/WiBro 단말과 같은 비 UICC 단말기들을 고려하여 UICC를 사용하지 않고도 높은 안전성과 편리한 이동성 및 휴대성이 제공되는 EAP-AKA를 제안한다. 제안 프로토콜은 UICC와 같은 스마트 카드를 사용하는 대신 DH (Diffie-Hellman) 키 교환 암호 알고리즘과 사용자의 패스워드를 사용한다. 제안 기법은 기존 WLAN/WiBro 단말들에게 스마트 카드 리더기와 같은 하드웨어적인 장치 장착을 요구하지 않고, 기존의 3GPP 인증 구조를 크게 변경하지 않고, WLAN 및 WiBro 단말에게 UICC 방식의 EAP-AKA와 같은 수준의 안전성과 휴대성을 제공하기 때문에 이질적인 무선 네트워크에서 상호 인증 연동이 용이하다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 이질적인 네트워크 인증 연동에 대한 기존 기법들을 살펴보고, Ⅲ장에서 제안하는 비 UICC 방식의 EAP-AKA 인증 절차와 제안 기법을 이용한 3GPP 및 WLAN, WiBro 망에서 핸드오버 인증 과정을 살펴보고, Ⅳ장에서 제안하는 인증 방법의 안전성, 휴대의 편리성, 이동 단말의 성능을 분석하고, 기존 기법들과 비교 분석한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 기술 및 문제점 분석

3GPP, WLAN, WiBro 무선 네트워크 간에 인증 연동에 대한 연구는 EAP-AKA 방식과 비 EAP-AKA 방식으로 나뉜다.

3GPP 표준에서는 WLAN과의 인증 연동을 위하여 UICC를 사용하는 EAP-AKA를 인증 연동 기술로 표준화하였다[6]. WLAN 사용자들은 3GPP 홈 네트워크의 AAA 인증 서버와 EAP-AKA 통신을 통해 인증 서비스를 받는다. 또한 3GPP 표준에서는 EAP-AKA long-term 비밀키가 WLAN 단말기와 분리되어 UICC에 저장될 것을 요구한다. *Tsai* 등은 SIM (Subscriber Identity Module) 기반의 인증으로 GSM/GPRS와 WLAN 간 인증 연동 기술을 제안하였다[7]. 제안 기술이 GSM과 WLAN 간 SIM 기반의 인증이지만, 기본 원리를 3GPP와 WLAN 간 인증 연동을 위하여 사용할 수 있다. *Zivkovic* 등은 3G/WLAN의 loosely coupled 구조에서 EAP-AKA 및 다양한 EAP 인증 기술들을 통합하여 SSO (Single Sing On) 방식의 원리를 이용한 인증 연동 방식을 제안하였다[8]. 모바일 단말은 EAP-TLS, EAP-TTLS, EAP-SIM, EAP-MD5 등 다양한 EAP 기반의 인증 모듈들을 설치하고, 단말이 이질적인 네트워크를 이동할 때마다 액세스 네트워크에서 요구하는 인증 방법을 모바일 단말에 설치된 SmartClient 모듈이 사용자의 개입 없이 적절한 인증 방식을 선택하여 인증 절차를 수행한다. *Zivkovic*의 기법에서는 단말의 초기 인증 과정에서 생성된 마스터 키를 서로 다른 인증 방법에서도 공유하기 때문에 각 인

증 기법들은 마스터 키를 생성하기 위한 추가 절차가 필요하지 않다. WiBro 무선 네트워크와 3GPP 네트워크 간의 인증 연동을 위하여 WiBro에서 UICC 기반의 EAP-AKA 적용에 대한 연구도 진행되었다[9]. 앞서 설명한 EAP-AKA 방식들은 모두 WLAN/WiBro 단말에서 UICC 장착을 요구한다.

그러나 기존 비 UICC 단말들이 EAP-AKA를 적용하기 위해서는 UICC를 하드웨어적으로 추가 장착해야 하는 비용 부담이 있고, 구조적으로 UICC를 장착할 수 없는 이동 단말들도 있기 때문에 이를 고려하여 UICC를 사용하지 않는 EAP-AKA 방식도 연구가 되었다[10]. 비 UICC 단말기에서의 EAP-AKA 인증 처리 방법은 이동 단말기에 128 비트의 long-term 비밀키를 UICC에 저장하는 대신 단말기에 안전하게 저장하기 위하여, 사용자의 패스워드와 랜덤 값을 사용한다. 사용자의 패스워드는 long-term 키를 암호화 및 복호화하는 비밀키로 사용된다. 그러나 패스워드를 사용하여 long-term 비밀키를 암호화하여 단말에 저장하는 방식은 long-term 비밀키가 단말에 저장되기 때문에 비밀 정보 저장에 있어서 매체 분리 원칙이 어긋나 안전성이 떨어지고, 단말이 바뀔 경우 long-term 비밀키를 이동시키거나 새로 할당받아야 하기 때문에 휴대성 및 이동성에 있어서 불편함이 있다.

EAP-AKA를 사용하지 않는 방식으로는, *Yang* 등이 부인 방지 기능을 제공하기 위하여 공개키 알고리즘을 이용한 인증 방식을 제안하였다[11]. EAP-AKA 방식은 기본적으로 UE (User Equipment)와 HSS/HLR (Home Subscriber Service/Home Location Register)간에 공유한 128 비트의 long-term 공유키를 기반으로 이루어지기 때문에 부인 방지 기능이 제공되지 않는다. 이는 3GPP 홈 네트워크와 방문 네트워크 간에 과금 문제를 일으킬 수 있다. 또한 *Tseng* 등도 3GPP와 WLAN 연동 네트워크에서 OTP (One Time Password)를 사용한 간단하고 효율적인 인증 프로토콜과, 부인 방지 기능을 제공하기 위하여 공개키 알고리즘을 이용한 과금 및 인증 프로토콜을 제안하였다[12]. *Kambourakis* 등은 3GPP/WLAN 연동 네트워크에서 양단간 보다 강한 보안 및 인증을 제공하기 위하여 PKI 기반 구조의 EAP-TLS 인증 프로토콜을 제안하였다[13]. 3GPP와 WLAN 네트워크 연동에서 부인 방지 기능을 제공하기 위하여 공개키 알고리즘을 사용한 인증 방식을 제안하고 있지만, PKI 구축 문제로 인해 현실적으로 적용하기 어렵다. 또한 기존 3GPP 인증 시스템을 변경해야 하는 문제도 있다.

이와 같이 3GPP 시스템 중심으로 WLAN 및 WiBro 네트워크가 연동되는 환경에서 EAP-AKA 인증과 비 EAP-AKA 인증 기법들이 다양하게 제안되었지만, 새로운 인증 구조 도입으로 인증 시스템 변경 및 설치에 따른 추가 비용 없이 이미 폭 넓게 설치되어 안정적으로 운영되고 있는 3GPP의 EAP-AKA를 사용하는 것이 바람직하다. 그러나 UICC 장착 비용 문제 및 단말의 구조적인 문제 때문에 UICC를 사용하지 못하는 단말들이 EAP-AKA를 사용할 때는 다음과 같은 사항을 고려해서 비 UICC 단말들에게도 안전하고 편리한 이동성 및 휴대성을 제공해 줄 수 있는 EAP-AKA 인증 방법이 필요하다.

- Long-term 비밀키 저장에 대한 안전성

3GPP 표준에서는 EAP-AKA 인증 기법 사용시 UICC 사용을 권장하고 있다. EAP-AKA의 핵심 비밀키인 128 비트의 long-term 비밀키를 보다 안전하게 저장하기 위하여 단말과 분리된 UICC 매체에 long-term 비밀키를 저장하도록 권고하고 있다. 따라서 비 UICC 단말이 EAP-AKA 인증 기법을 사용할 때 매체 분리 원칙에 입각한 long-term 비밀키 저장과 같은 안전성을 제공해야 한다.

- UICC와 같은 편리한 이동성 및 휴대성

UICC와 같은 스마트 카드 형태는 사용자에게 있어서 편리한 이동성 및 휴대성을 제공한다. 예를 들어, 이동 단말이 바뀔 경우, 사용자의 인증 정보 및 비밀 정보를 UICC만 새로운 단말에 장착하기만 하면 이동시킬 수 있다. 따라서 비 UICC 단말이 EAP-AKA 인증 기법을 사용할 때 인증 및 중요 정보에 대해서 편리한 이동성 및 휴대성이 제공되어야 한다.

III. 제안 기법

그림 1은 3GPP 표준에서 제안한 3G/WLAN 인증 연동 구조를 본 논문에서 WLAN/WiBro 연동 구조로 확장하고 제안 기법을 적용한 인증 연동 구조이다. 제안 기법은 UICC 방식에서 인증 벡터를 생성하기 위한 128 비트의 long-term 비밀키를 대신하여 UE와 HSS/HLR 간에 DH 키 교환 알고리즘을 통해 생성된 DH 세션키

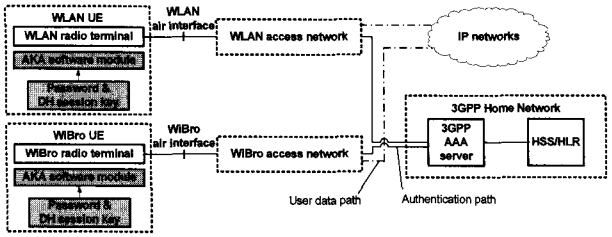


그림 1. 3GPP 기반의 WLAN/WiBro 인증 연동 구조
Fig. 1. Authentication architecture of WLAN/WiBro based on 3GPP system.

를 인증 벡터 생성을 위한 short-term 마스터 키로 사용한다. 또한 인증과 이동 및 휴대의 편리성을 제공하기 위하여 사용자의 패스워드를 사용한다. 제안 기법을 적용할 경우 기존의 WLAN 또는 WiBro 단말들은 3GPP AAA 서버와 인증을 수행하기 위하여 DH 알고리즘과 패스워드, EAP-AKA 알고리즘 소프트웨어 모듈만을 필요로 한다.

1. 비 UICC 방식의 EAP-AKA 인증

본 절에서는 3GPP에서 정의한 UICC 기반의 EAP-AKA 표준[6] 절차 중, 제안 기법을 적용하기 위하여 수정된 일부 절차 (단계 3, 5-11, 15)에 대해서 설명한다. 나머지 다른 인증 단계는 3GPP의 EAP-AKA[6] 절차와 동일하다. 제안 기법에서 사용되는 파라미터들을 표 1에 정의하였다.

표 1. 표기법
Table 1. Notation.

표 기	정 의
$H(\ )$	안전한 일방향 해쉬함수
pwd	패스워드
$\|\|$	두 개의 비트열의 연접
p	큰 소수
Z^*_p	모듈러 p로의 곱셈군
x, y, s	Z^*_p 속하는 랜덤 값
g	Z^*_p의 생성자
$K_{X\text{-}Y}$	X와 Y 노드 사이에서 DH 세션키
$Time$	현재 시간
$R\text{-}flag$	인증 벡터 생성 요청 플래그

먼저, HSS/HLR은 사용자 데이터베이스에 패스워드를 $H(pwd)$과 $g^{H(pwd)} \bmod p$ 형태로 저장한다고 가정한다. UE는 그림 2의 단계 3을 시작할 때 식 (1)과 같이 M_1 값을 생성하고, 단계 3-5를 거쳐 M_1 값을 AAA 인증 서버에게 전달한다.

$$M_1 = g^x \bmod p \oplus H(pwd) \tag{1}$$

단계 6에서 AAA 서버는 M_1 값을 HSS/HLR에게 전달하고, HSS/HLR은 UE의 IMSI를 확인하고 해당하는 $H(pwd)$를 사용하여 UE의 DH 공개키 $g^x \bmod p$를 계산하고, 임의의 랜덤 값 s를 선택하여 DH 세션키

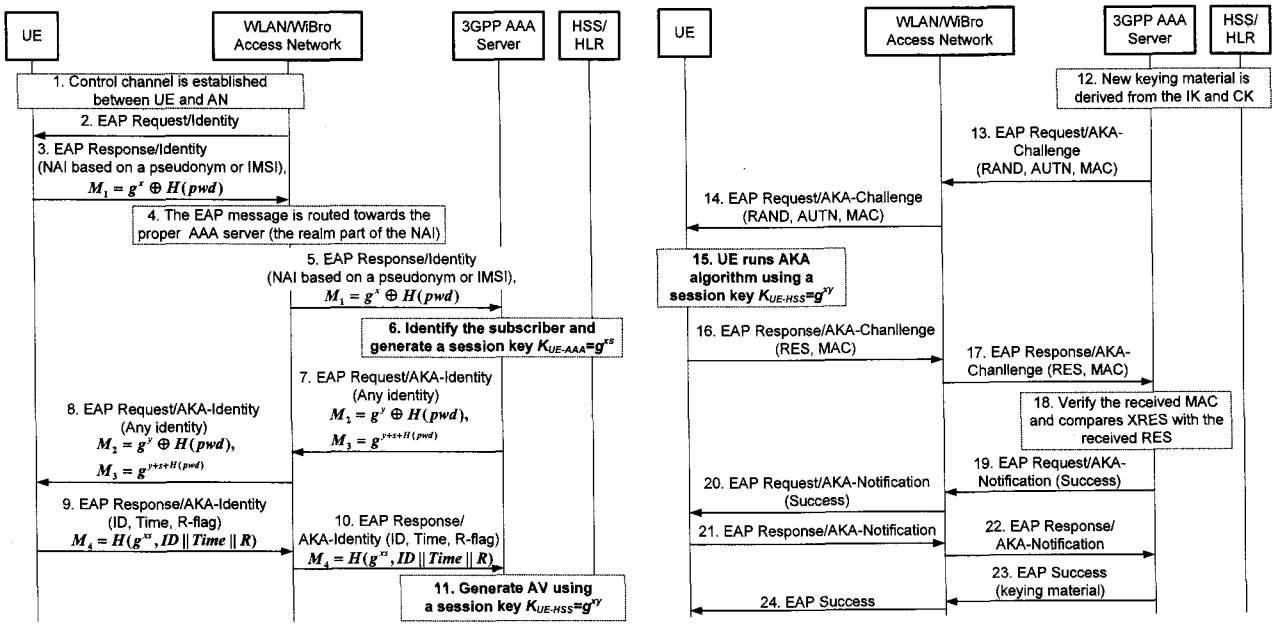


그림 2. 비 UICC 방식의 EAP-AKA 인증 절차
Fig. 2. EAP-AKA message flow based on non-UICC.

$K_{UE\text{-}AAA}=g^{xs}\bmod p=(g^{x}\bmod p)^{s}\bmod p$ 계산한다. 또한 식 (2)와 같이 M_2와 M_3를 생성하여 $K_{UE\text{-}AAA}$와 함께 AAA 인증 서버에게 보안 채널을 통해 안전하게 전달한다. AAA 인증 서버는 $K_{UE\text{-}AAA}$를 안전하게 저장하고, 값 M_2와 M_3를 단계 7-8을 통해 UE에게 전달한다.

$$M_2 = g^{y}\bmod p \oplus H(pwd),\quad M_3 = g^{y+s+H(pwd)}\bmod p \tag{2}$$

UE는 M_2 메시지와 $H(pwd)$를 사용하여 HSS/HLR의 DH 공개키 $g^{y}\bmod p$를 계산하고, M_3로부터 $g^{s}\bmod p$ 값을 추출한다. 또한 UE는 DH 비밀키 x를 사용하여 DH 세션키 $K_{UE\text{-}AAA}=g^{xs}\bmod p=(g^{s}\bmod p)^{x}\bmod p$를 계산한다. UE는 식 (3)과 같이 값 M_4를 생성한 후, {ID, Time, R-flag} 값과 함께 단계 9와 10을 거쳐 AAA 서버에게 전송한다.

$$M_4 = H(g^{xs}\bmod p, ID\|Time\|R) \tag{3}$$

여기서, R-flag는 사용자가 단말을 변경하여 두 개의 DH 세션키 ($K_{UE\text{-}AAA}$, $K_{UE\text{-}HSS}$)를 저장하고 있지 않은 경우에 HSS/HLR에게 DH 키 교환 과정을 통해 두 개의 DH 세션키 생성을 요청하는 플래그이다. R-flag의 사용 목적은 Ⅲ장 2절에서 자세히 설명한다.

단계 11에서 M_4 메시지를 수신하면, AAA 서버는 저장하고 있던 $K_{UE\text{-}AAA}$를 사용하여 M_4 값을 검증한다. 참고로, $K_{UE\text{-}AAA}$를 포함하는 M_4 값은 공격자가 UE와 AAA 서버 사이에서 R-flag를 임의 조작하여 AAA 인증 서버가 불필요하게 인증 벡터 생성을 HSS/HLR에게 요청하는 과정을 차단하기 위한 목적이다. 검증이 성공적으로 이루어지면, AAA 서버는 R-flag 값과 AAA 서버 데이터베이스에 UE를 위해 사용할 수 있는 인증 벡터의 존재 유무에 따라 HSS/HLR에게 인증 벡터를 요청한다. Ⅲ장 2절의 표 2에 따라 AAA 인증 서버가 HSS/HLR에게 인증 벡터를 요청할 필요가 없으면, AAA 서버는 {RAND, AUTN}으로 구성된 하나의 인증 벡터와 MAC (Message Authentication Code) 값을 UE에게 전송하여 UE와 EAP-AKA 표준 인증[6] 절차를 수행한다. 만약, AAA 인증 서버가 HSS/HLR에게 인증 벡터를 요청할 필요가 있어 HSS/HLR에게 새로운 n개의 인증 벡터를 요청하면, HSS/HLR 서버는 UE의 DH 공개키 $g^{x}\bmod p$과 자신의 DH 개인키 y를 사용하여 인증 벡터 생성을 위한 DH 세션키 $K_{UE\text{-}HSS}=g^{xy}\bmod p=(g^{x}\bmod p)^{y}\bmod p$를 생성한다. HSS/HLR은 $g^{xy}\bmod p$를

표 2. R-flag 사용
Table 2. Usage of R-flag.

R-flag	AAA	DH 키 교환 수행 여부
False (두 개의 DH 세션 키 $K_{UE\text{-}AAA}$, $K_{UE\text{-}HSS}$ 있음)	사용할 인증 벡터 있음	표준 EAP-AKA 절차[6] 수행
	사용할 인증 벡터 없음	새로운 인증 벡터 생성 (DH 키 교환 과정 수행)
True (두 개의 DH 세션 키 $K_{UE\text{-}AAA}$, $K_{UE\text{-}HSS}$ 있음)	사용할 인증 벡터 있음	
	사용할 인증 벡터 없음	

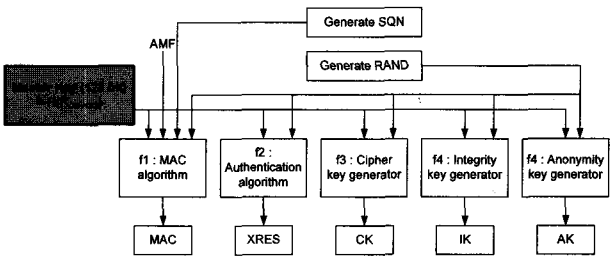


그림 3. HSS/HLR에서 $K_{UE\text{-}HSS}$를 이용한 인증벡터 생성
Fig. 3. Generation of authentication vectors using DH session key $K_{UE\text{-}HSS}$ on the HSS/HLR.

해쉬하여 128 비트의 short-term 비밀키를 생성하고 n 개의 인증 벡터들을 생성하기 위하여 3GPP AKA 알고리즘들을 ($f1$, $f1^{*}$, $f2$, $f3$, $f4$, $f5$, $f5^{*}$) 그림 3과 같이 수행한다. 마지막으로 HSS/HLR은 생성된 n 개의 인증 벡터들을 AAA 서버에게 전송한다. AAA 서버는 n 개의 인증 벡터들을 저장하고, 단계 13-14를 통해 인증 벡터 파라미터들을 UE에게 전달한다.

단계 15에서, UE는 수신한 인증 벡터 파라미터를 검증하기 전에 UE가 저장하고 있는 HSS/HLR의 DH 공개값 $g^{y}\bmod p$과 자신의 DH 개인키 x를 사용하여 DH 세션키 $K_{UE\text{-}HSS}=g^{xy}\bmod p=(g^{y}\bmod p)^{x}\bmod p$를 생성한다. UE는 $g^{xy}\bmod p$를 해쉬하여 128 비트의 short-term 비밀키를 생성하고, 그림 4와 같이 short-term 비밀키를

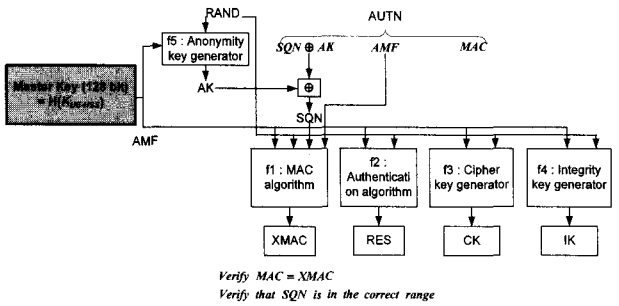


그림 4. UE에서 $K_{UE\text{-}HSS}$를 이용한 인증벡터 생성
Fig. 4. Generation of authentication vectors using DH session key $K_{UE\text{-}HSS}$ on the UE.

AKA 알고리즘의 마스터키로 사용하여 인증 벡터를 생성하고 AAA 서버로부터 수신한 인증 벡터 {RAND, AUTN} 값과 MAC 값을 검증한다. 검증이 성공적으로 이루어지면, UE는 생성된 인증 벡터 {RES}와 MAC 값을 3GPP AAA 서버에 전달하여 인증을 받는다. 단계 16부터 24까지는 3GPP 표준 문서의 EAP-AKA 절차를 따른다.

UE는 생성된 두 개의 DH 세션키 $K_{UE\text{-}AAA}$와 $K_{UE\text{-}HSS}$를 저장하고, 이후 EAP-AKA 과정에서 일정 기간 동안 재사용한다.

2. DH 세션키 동기화 (R-flag)

제안 기법은 UE에서 두 개의 DH 세션키가 저장되어 있는지 여부와 AAA 인증 서버에서 UE를 위해 사용할 인증 벡터가 존재하는지 여부에 따라서 AAA 인증 서버가 HSS/HLR에게 새로운 인증 벡터 생성을 (DH 키 교환 과정 수행) 요청할 것인지를 결정한다. 표 2는 UE의 R-flag와 AAA 인증 서버의 인증 벡터 저장 상태에 따라 UE와 HSS/HLR이 어떤 경우에 DH 키 교환 과정을 수행하고 인증 벡터를 생성해야 하는지를 보여준다.

UE가 이전의 EAP-AKA 과정을 통해 두 개의 DH 세션키를 저장하고 있다면, 단계 3에서 새로운 DH 비밀키 x'으로 생성된 M_1' 메시지, 저장하고 있는 $K_{UE\text{-}AAA}$를 사용하여 생성한 M_4' 메시지와 {ID, Time', R(False)} 값들과 함께 AAA 서버에게 전달한다. AAA 서버는 저장하고 있는 $K_{UE\text{-}AAA}$를 사용하여 M_4' 메시지를 검증한다. AAA가 UE를 위해 사용할 인증 벡터를 저장하고 있는 경우에는, M_2, M_3 메시지 생성 및 전달 과정 없이 임의의 인증 벡터 하나를 선택하여 UE와 함께 EAP-AKA 표준 인증 절차를 수행한다. 만약, AAA가 UE를 위한 인증 벡터를 저장하고 있지 않으면, M_1 메시지를 HSS/HLR에게 전달하고, UE와 HSS/HLR이 기존의 DH 세션키 대신에 새로운 DH 세션키 {$K_{UE\text{-}AAA}'$, $K_{UE\text{-}HSS}'$}로 갱신하고, 새로운 인증 벡터를 생성하도록 유도한다.

UE가 두 개의 DH 세션키를 저장하고 있지 않다면, 그림 2와 같은 단계를 따른다.

3. 제안 기법을 이용한 핸드오버 인증 구조

UICC를 사용하지 않는 EAP-AKA 방식을 제안함으로써 3GPP, WLAN, WiBro 망에서 UE들은 모두 EAP-AKA 인증을 수행할 수 있게 되었다. 이와 같이 서로 다른 이기종 망에서 동일한 인증 메커니즘을 사용하는 것은 이기종 망 간 핸드오버시에도 동일한 네트워크 내에서 핸드오버 인증을 수행하는 것과 같은 효과를 얻을 수 있다.

본 논문에서는 그림 5와 같이 이질적인 네트워크에

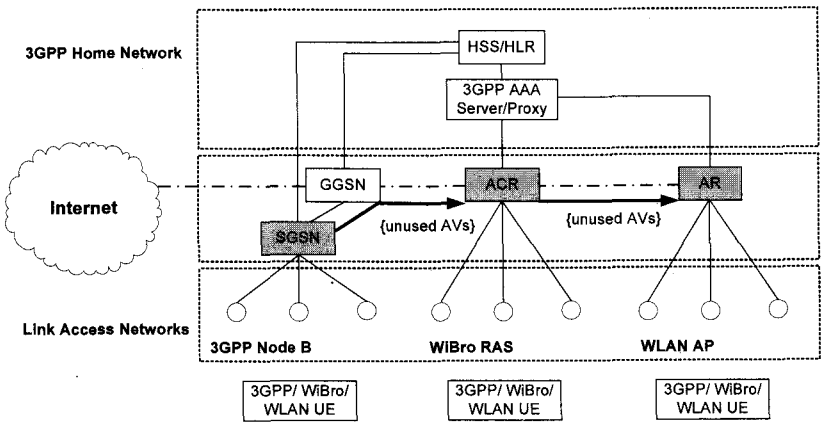


그림 5. EAP-AKA 기반의 핸드오버 인증 구조
Fig. 5. Architecture of handover authentication based on EAP-AKA.

서 EAP-AKA를 사용한 핸드오버 인증 구조에 대해서 살펴본다. 먼저 WiBro 및 WLAN 네트워크에서는 인증 벡터들을 네트워크 계층의 ACR (Access Conrtol Router) 또는 AR (Access Router)에서 관리하고, 인증 벡터들을 관리하는 노드들 간에는 (3GPP-SGSN, WiBro-ACR, WLAN-AR) 안전한 채널이 설정되어 있는 상황을 가정한다. 이런 조건에서 EAP-AKA 기반의 핸드오버 인증은 SCT (Security Context Transfer) 방식을 사용하여 각 네트워크 간에 사용하지 않은 인증 벡터들을 (unused AVs) 전달해 줌으로써 간단하게 핸드오버 인증을 수행할 수 있다.

Ⅳ. 제안 기법 분석 및 비교

제안 기법은 기존 WLAN/WiBro 단말들이 UICC 기능을 추가하기 위해 요구되는 비용 문제 및 구조적인 문제로 UICC를 사용하지 않고 EAP-AKA를 사용할 때, UICC의 안전성 및 편리한 이동성과 휴대성을 보장하지 못하는 문제점을 해결하였다. UICC를 사용하는 EAP-AKA는 128비트의 long-term 비밀키가 사용자 단말과 분리되어 UICC에 저장되기 때문에 높은 안전성이 보장되고, UICC를 사용하고자 하는 단말에 쉽게 장착하여 사용할 수 있기 때문에 편리한 이동성 및 휴대성이 제공된다. 본 논문에서는 UICC를 사용하는 대신 DH 알고리즘과 패스워드를 사용한 EAP-AKA를 제안했기 때문에, UICC를 사용했을 때와 동일한 보안 수준 및 편리한 이동성과 휴대성을 제공한다. 또한 short-term 비밀키를 사용하여 인증 벡터를 생성하기 때문에 기존 기법에서 제공하지 않던 long-term 비밀키에 대한 PFS (Perfect Forward Secrecy)와 PBS (Perfect Backward Secrecy) 기능도 제공한다. 마지막으로, 기존 3GPP EAP-AKA 인증 구조를 크게 수정하지 않고 3GPP 시스템 중심의 WLAN/WiBro 인증 연동 구조에서 기존 단말들에 쉽게 적용이 가능하다. 다음에서 제안 기법의 보안, 편리한 이동성 및 휴대성, DH 알고리즘 적용에 따른 단말 자원의 성능 부분을 분석하고, 기존 기법과 비교하였다.

1. 안전성 및 이동성, 성능 분석

가. 안전성 분석

제안 기법과 같이 패스워드를 사용하는 인증 및 키 교환 프로토콜에서 가장 큰 보안 문제는 패스워드에 대한 사전 공격들이다. 사전 공격은 메시지 스니핑을 이용한 공격, 위장 공격을 이용한 공격, 데닝 사코 공격을 이용한 공격으로 분류할 수 있다. 먼저, 공격자가 패킷 스니핑을 통해 UE와 AAA 서버 간에 교환하는 메시지를 통해 사전 공격을 수행할 수 있다. 그러나 공격자는 안전한 일방향 해쉬 함수, 랜덤 값, DLP (Discrete Logarithm Problem) 등으로 보호되어 있는 사용자의 패스워드를 공개된 메시지들로부터 추측할 수 없다. 또한 제안 기법은 정상적인 UE 또는 HSS/HLR인 것처럼 위장하여 인증을 요청한 후 응답해 오는 인증값을 사용한 사전 공격에도 안전하다. 예를 들어, 공격자가 UE로 위장하여 임의의 패스워드 pwd'를 사용해 M_1'을 생성하고 HSS/HLR 서버에게 전송한다고 가정하자. AAA 서버는 HSS/HLR로부터 수신한 $K_{UE\text{-}AAA}'$를 사용하여 단계 10에서 수신한 M_4' 메시지를 검증하는데 실패하고, EAP-AKA 인증 과정을 종료한다. 따라서 UE로 위장한 공격자는 사전 공격을 수행할 수 없다. 반대로, 공격자가 HSS/HLR로 위장할 경우에, 공격자는 임의의 패스워드 pwd'를 사용해 M_2'와 M_3' 메시지를 생성해 UE에게 전달한다. UE가 M_4 값을 생성하여 인증 서버로 위장한 공격자에게 전송하지만, 공격자는 UE의 DH 비밀키 x를 모르기 때문에 사전 공격을 수행할 수 없다. 데닝 사코 공격은 임의의 세션키가 공격자에 의해서 노출되었을 때, 공격자가 사용자의 패스워드 또는 또 다른 임의의 세션키를 알아낼 수 있는 공격이다. 제안 기법은 패스워드와 DH 세션키가 어떤 관계를 갖지 않고 독립적으로 생성되기 때문에 데닝 사코 공격에 대해서도 안전하다.

많은 암호학적 연산 수행을 통한 DoS 공격 또한 네트워크 보안 프로토콜 설계시 고려되어야 한다. 제안 기법은 DH 알고리즘 사용으로 기존 EAP-AKA 방법보다 서버에서 지수 연산에 대한 오버헤드가 발생한다. 제안 기법은 DH 키 교환 과정을 3장 2절에서와 같이 UE에서 DH 세션키들의 저장 유무와 AAA 인증 서버에서 UE에 대한 인증 벡터 저장 유무에 따라서 수행하게 된다. 따라서 공격자가 UE의 DH 세션키 저장 유무를 표시하는 R-flag 값을 항상 "False" 값으로 조작하여 AAA 서버가 HSS/HLR 서버에게 DH 키 교환 과정을 유도할 수 있다. 그러나 제안 기법은 $K_{UE\text{-}AAA}$를 사용하여 R-flag에 대해서 무결성을 제공하기 때문에 공격자가 R-flag 값을 조작할 수 없다. 따라서 제안 기법은 서버의 암호학적 연산량 과부하를 이용한 DoS 공격

에 안전하다.

제안 기법은 새로운 인증 벡터 생성 요청시 UE와 HSS/HLR에서 새롭게 생성되는 임의의 값인 DH 개인키 x, y와 현재 *Time* 값이 사용되기 때문에 재전송 공격에 대해서 안전하다. 또한 제안 프로토콜은 UE와 HSS/HLR 간에 비밀정보인 패스워드와 해쉬함수를 사용하기 때문에 MITM (Man in the Middle) 공격에 대해서도 안전하다.

마지막으로, PFS와 PBS는 인증 및 키 교환 프로토콜에서 중요한 보안 특성이다. 기존 EAP-AKA에서는 공격자가 UICC를 획득하게 될 경우, 물리적인 접근을 통해서 저장된 long-term 비밀키를 획득할 수 있다. 이런 경우 공격자는 long-term 비밀키로부터 데이터 보호를 위한 이전 및 이후의 모든 세션키들을 알아낼 수 있다. 그러나 제안 기법은 HSS/HLR이 인증 벡터를 생성할 때마다 $K_{UE\text{-}HSS}$를 이용한 short-term 키를 사용하기 때문에 기존의 인증 기법보다 향상된 PFS 및 PBS를 제공한다. 즉, 제안 기법에서는 short-term 키가 노출될 경우 노출된 short-term 키로부터 유도된 인증 벡터 값과 세션키 (IK, CK)들만 노출되고, 이전 및 이후의 short-term 키로부터 생성되는 인증 벡터와 세션키에 대해서는 안전하다.

나. 편리한 이동성 및 휴대성

제안 프로토콜은 3GPP 시스템 기반의 EAP-AKA 인증과 같이 동일하게 휴대의 편리성 및 로밍 기능을 제공한다. 제안 기법에서 패스워드는 사용자가 쉽게 기억할 수 있는 특성 때문에 UICC 없이도 사용자가 언제 어디서나 임의의 UE를 사용하여 인증 받을 수 있다. 한편, 제안기법에서는 UICC를 사용하지 않기 때문에 사용자가 패스워드뿐만 아니라 IMSI (International Mobile Subscriber Identity)도 기억해야 하는 불편함이 있다. 그러나 사용자는 14~16자리 수로 (3자리 : 국가 코드, 2~3자리 : 네트워크 사업자 코드, 9~10자리 : 사용자 식별 번호) 구성된 IMSI 중에서 일반적으로 사용자의 식별 코드 값 9~10자리의 수만을 기억하면 되기 때문에 크게 문제되지 않는다. 글로벌 로밍 기능은 기존의 EAP-AKA 인증과 같이 외부 네트워크에서 패스워드를 기억하고 있는 사용자가 3GPP AAA 프락시 서버를 통해서 인증을 받을 수 있기 때문에 가능하다.

다. UE에서 DH 알고리즘으로 인한 오버헤드 분석

제안 프로토콜은 DH 알고리즘을 사용하기 때문에 CPU 성능이나 전력 등이 충분치 않은 이동 단말에서 DH 지수 모듈러 계산에 따른 오버헤드가 발생한다. 그러나 UE는 매 인증시 DH 지수 계산을 수행하는 것이 아니라 UE가 DH 세션키를 저장하고 있지 않거나 3GPP AAA 서버가 UE에 대해서 저장하고 있는 인증 벡터 값이 없을 때만 HSS/HLR과 DH 알고리즘을 수행하기 때문에 UE에게 큰 부담이 되지 않는다. UE가 DH 세션키를 저장하고 있고 AAA 인증 서버가 UE를 위한 인증 벡터를 저장하고 있다면, UE는 DH 키 교환 과정

표 3. EAP-AKA 방식 비교
Table 3. Comparison of EAP-AKA schemes.

	3GPP 표준[6]	*Tsai* 등의 기법[7]	*Zivkovic* 등의 기법[8]	WiBro EAP-AKA방식[9]	비 UICC 방식[10]	제안 기법
네트워크 연동 환경	3GPP/WLAN	GSM/WLAN	3GPP/WLAN	3GPP/WiBro	3GPP/WLAN/ WiBro	3GPP/WLAN/ WiBro
기존 UE에서 요구사항	UICC 장착 또는 스마트 카드 리더기	UICC 장착 또는 스마트 카드 리더기	UICC 장착 또는 스마트 카드 리더기, SmartClient 모듈	UICC 장착 또는 스마트 카드 리더기	EAP-AKA 소프트웨어 모듈	EAP-AKA 소프트웨어 모듈
휴대성	좋음 (UICC)	좋음 (UICC)	좋음 (UICC)	좋음 (UICC)	불편 (단말에 저장)	좋음 (패스워드)
공유 비밀키	long-term	long-term	long-term	long-term	long-term	short-term
PFS 및 PBS	지원 안됨	지원 안됨	지원 안됨	지원 안됨	지원 안됨	지원함
암호 알고리즘	AKA 함수	AKA 함수	AKA 함수	AKA 함수	AKA 함수	AKA 함수, DH

없이 AAA 서버와 함께 EAP-AKA 인증 과정만 수행하기 때문에 DH 지수 모듈러 계산에 따른 오버헤드가 큰 부담이 되지 않는다.

2. 기존 EAP-AKA 방식과 비교 분석

EAP-AKA 인증 방법을 사용하는 기존 기법들과 제안 기법을 비교하여 표 3에 정리하였다. 기존에 제안된 EAP-AKA 인증 연동 방법들은 3GPP(또는 GSM)와 WLAN 네트워크 연동 구조에 주로 초점이 맞춰져 연구 되었지만, 기본 인증 연동 원리를 WiBro 네트워크에도 쉽게 적용할 수 있다. 단, 기존의 이동 단말기에서 UICC를 장착해야 하거나 스마트 카드 리더기 설치와 같은 하드웨어적인 요구사항이 필요하다. 이러한 문제를 해결하기 위하여 제안 기법과 비 UICC 방식이[10] 3GPP/WLAN/WiBro 네트워크 연동 환경에서 EAP-AKA 소프트웨어 알고리즘 모듈만을 이동 단말에 탑재하여 사용될 수 있도록 제안되었다.

편리한 이동성 및 휴대성 측면에서는 UICC 방식과 패스워드 방식으로 분리하여 비교할 수 있다. UICC 방식의 EAP-AKA에서 사용자는 UICC를 사용하고자 하는 이동 단말에 이동 장착만 하면 IMSI 및 128 비트의 long-term 비밀키가 쉽게 새로운 단말로 옮겨진다. 패스워드 방식의 EAP-AKA는 UICC와 같이 물리적인 칩을 휴대할 필요 없이 사용자가 기억하고 있는 패스워드만 있으면 언제 어디서나 새로운 단말에서 EAP-AKA를 수행할 수 있다. 비 UICC 방식의[10] 경우 단말에 128 비트의 long-term 비밀키를 저장하고, 이 키를 보다 안전하게 저장하기 위하여 사용자의 패스워드로 암호화하여 저장하기 때문에, 만약 새롭게 단말이 바뀐다면 사용자는 128 비트의 long-term 비밀키를 옮기거나 새롭게 할당받아야 하는 번거로움이 있다. 그러나 제안 기법은 패스워드 뿐만 아니라 인증 벡터를 생성하기 위한 마스터 키 생성 또한 DH 알고리즘으로 일시적으로 생성하기 때문에 사용자가 128 비트의 short-term 비밀키를 기억 및 이동할 필요가 없다.

EAP-AKA 인증 방법들의 안전성 측면에서 비교해 보면 다음과 같다. 제안 기법을 제외한 다른 인증 방법들은 모두 128 비트의 long-term 비밀키를 사용하기 때문에, UICC 분실 등으로 비밀키가 노출 될 경우 데이터 보호를 위한 이전 및 이후 세션키에 대해서 PFS와 PBS를 제공하지 못한다. 그러나 제안 기법은 short-term 비밀키를 사용하기 때문에 기존의 인증 방법보다 향상된 PFS와 PBS 기능을 제공한다.

마지막으로, 기존의 EAP-AKA 인증은 AKA 함수만 사용하지만, 제안 기법에서는 AKA 함수 이외에 DH 알고리즘을 사용하기 때문에 UE 및 HSS/HLR에서 지수 연산에 대한 부담이 존재할 수 있다. 그러나 제안 기법에서는 UE와 HSS/HLR이 새로운 인증 벡터를 생성할 때만 DH 지수 계산을 수행하기 때문에 UE와 HSS/HLR 서버에게 큰 부담이 되지 않는다.

V. 결 론

본 논문에서는 3GPP 시스템 기반의 WLAN 및 WiBro 연동 환경에서 원활한 인증 연동을 위하여 UICC를 사용하지 않는 EAP-AKA 인증 방법을 제안하였다. 3GPP 시스템 중심의 WLAN/WiBro 네트워크 연동 환경에서 다양한 인증 연동 연구가 이루어지고 있지만, 3GPP의 인증 연동 기술인 UICC 방식의 EAP-AKA는 기존의 WLAN/WiBro 단말들에게 UICC 장착을 요구한다. 제안 기법은 UICC 방식의 EAP-AKA가 갖는 안전성과 편리한 이동성 및 휴대성을 UICC 없이 제공하기 위하여 패스워드와 DH 알고리즘을 사용하였다. 제안 프로토콜은 패스워드 사용으로 편리한 이동성 및 휴대성을 제공하고, DH 세션키로 생성된 short-term 키로 UICC에 저장되어 있는 long-term 비밀키와 같은 수준의 안전성과 함께 향상된 PFS 및 PBS를 제공한다. 또한, 기존의 3GPP EAP-AKA 인증 구조에서 큰 수정을 요구하지 않는다.

참 고 문 헌

[1] A. K. Salkintzis, "Interworking techniques and architectures for WLAN/3G integration toward 4G mobile data networks," *IEEE Wirel. Commun.*, Vol. 11, No. 3, pp. 50-61, June 2004.

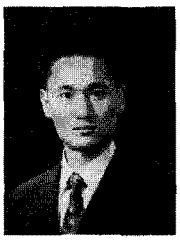
[2] K. Ahmavaara, H. Haverinen, and R. Pichna, "Interworking architecture between 3GPP and WLAN systems," *IEEE Commun. Mag.*, Vol. 41, No. 11, pp. 74-81, November 2003.

[3] G. Ruggeri, A. Iera, and S. Polito, "802.11-Based wireless-LAN and UMTS interworking: requirements, proposed solutions and open issues," *Comput. Netw.*, Vol. 47, No. 2, pp. 151-166, February 2005.

[4] ETSI TR 122 934 V7.0.0, Feasibility study on

3GPP system to Wireless Local Area Network (WLAN) interworking (Release 7), 3GPP Standard, 2007.
[5] F. Xu, L. Zhang, and Z. Zhou, "Interworking of Wimax and 3GPP networks based on IMS," *IEEE Commun. Mag.*, Vol. 45, No. 3, pp.144-150, March 2007.
[6] 3GPP TS 33.234, Wireless Local Area Network (WLAN) interworking security (Release 7), 3GPP Standard, 2006.
[7] Y. Tsai and C. Chang, "SIM-based subscriber authentication mechanism for wireless local area networks," *Comput. Commun.*, Vol. 29, No. 10, pp.1744- 1753, June 2006.
[8] M. Zivkovic, M. M. Buddhikot, K. Lagerberg, and J. van Bemmel, "Authentication across heterogeneous networks," *Bell Labs Tech. J.*, Vol. 10, No. 2, pp. 39-56, August 2005.
[9] 임선희, 이옥연, 전성익, 한진희, "EAP-AKA를 적용한 WiBro 무선 네트워크의 인증구조 연구," *한국통신학회논문지*, 제31권, 제4C호, pp. 441-450, 2006년 4월
[10] 정진화, 유성호, 비 유에스아이엠 단말기에서의 이에이피-에이케이에이 인증처리 장치 및 방법, 국내 특허 등록 10-2007-0041152, 2007년
[11] C.-C. Yang, Y.-W. Yang, and W.-T Liu, "A robust authentication protocol with non-repudiation service for integrating WLAN and 3G network," *Wirel. Pers. Commun.*, Vol. 39, No. 2, pp. 229-251, June 2006.
[12] Y.-M. Tseng, C.-C. Yang, and J.-H. Su, "Authentication and billing protocols for the integration of WLAN and 3G networks," *Wirel. Pers. Commun.*, Vol. 29, No. 3-4, pp. 351-366, June 2004.
[13] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking," *IEE Proc.-Commun.*, Vol. 151, No. 5, pp. 501-506, October 2004.
[14] G. M. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking," *IEEE Commun. Mag.*, Vol. 41, No. 11, pp. 82-88, November 2003.

저 자 소 개



최 재 덕(정회원)
2002년 숭실대학교 정보통신 전자공학부 학사.
2004년 숭실대학교 정보통신 공학과 석사.
2009년 숭실대학교 전자공학과 박사.
2004년 (주)애드팍테크놀러지 S/W 연구원
2009년~현재 숭실대학교 전자공학과 박사후 연구원
<주관심분야 : VoIP 보안, 차량 네트워크 보안, 이동 네트워크 보안>

정 수 환(평생회원)-교신저자
1985년 서울대학교 전자공학과 학사.
1987년 서울대학교 전자공학과 석사.
1996년 University of Washington 박사.
1988년~1991년 한국통신 전임 연구원
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교
2009년~현재 지식경제부 지식정보보안 PD
<주관심분야 : VoIP 보안, 차량 네트워크 보안, 이동 네트워크 보안, RFID/USN 보안>