한국산학기술학회논문지
Vol. 9, No. 3, pp. 727-733, 2008

안전한 WiBro 서비스를 위한 PSD(Power Support Device) 기반 인증 프로토콜

이기성[1*]

Power Support Device (PSD) Based Authentication Protocol for Secure WiBro Services

Gi-Sung Lee[1*]

요 약 사용자가 안전한 WiBro 서비스를 받기 위해서 사용자 단말과 ACR(Access Control Router) 간에 인증이 선행되어야 한다. 그렇지 않을 경우, 많은 공격 위험으로부터 노출될 수 있다. 따라서 한국정보통신기술협회(TTA)에서는 휴대인터넷(와이브로™) 서비스를 위한 상호 인증 절차 표준을 제정하였다. 이 표준 프로토콜은 PISIM(Portable Internet Subscriber Identity Module)을 이용하여 PE(Portable Equipment)와 ACR 간에 상호 인증을 수행한다. 그러나 표준은 인증에 필요한 메시지의 수가 대체적으로 많은 편이며 PISIM의 분실과 에러가 발생했을 경우에는 사용자는 무선인터넷 서비스를 사용할 수 없게 된다. 따라서 본 논문에서는 ACR과 PSS 간에 키 동의 프로토콜을 수행하여 PSS를 인증한다. 이때 PSS의 계산량을 지원하기 위한 PSD(Power Support Device)가 키 동의 프로토콜에 참여하게 된다. 이렇게 생성된 키는 ACR과 안전한 통신 세션을 맺고 있는 KAS(Key Authentication Server)에 PSS의 식별자와 키 정보를 암호화에서 저장한다. 끝으로 제안된 프로토콜의 안전성과 효율성을 분석한다.

Abstract An authentication between a user's terminal and a Access Control Router (ACR) is preceded so that a user receives secure WiBro services. Otherwise they can be exposed from many attack risks. So the Telecommunications Technology Association (TTA) constituted a mechanism of the mutual authentication for WiBro™ service. In mechanism a user executes the mutual authentication between a Portable Equipment (PE) and the ACR by using Portable Internet Subscriber Identity Module (PISIM). But this standard needs many message to authenticate the ACR and the users cann't use wireless Internet service. Therefore in this paper we propose the key agreement protocol between the PSS and the ACR to authenticate the PSS to ACR. At this time Power Support Device (PSD) for supporting the calculated quantity of the PSS is participated in the key agreement protocol. The ACR sends a generated key to Key Authentication Server (KAS) via secure IPsec tunnel and then it preserves the identity of the PSS and the value of key after it enciphered them. In conclusion we analyze the security and efficiency of the proposed protocol.

Key Words : WiBro, key agreement protocol, power support device (PSD), key authentication server (KAS)

1. 서론

WiBro 기술은 노트북, PDA, 휴대폰과 같은 이동 단말기 보급의 확산과 언제 어디서나 이동 중에도 다양한 단말기를 이용해서 높은 전송 속도로 무선인터넷 서비스를 필요로 하는 사용자들의 급증으로 인해 필요하게 되었으며 2007년 10월에 세계 최초로 3.5세대 IMT2000 국제 표준으로 채택되었다[1]. WiBro는 현재 상용화되는 이동성 지원 기술 중 가장 빠른 무선 전송속도를 제공하고 있으며 All-IP 기술을 채택함으로써 저렴한 비용을 기반으로 다양한 비즈니스 응용이 가능하다. WiBro 기술이 국제 표준으로 채택되기 이전에 한국정보통신기술협회에서는 2006년에 WiBro 기술과 관련된 몇 개의 표준을 정의했다. 먼저, "WiBro 기술에서의 IPv6 기술(IPv6 over WiBro)"은 와이브로 네트워크 상에서의 IPv6 오퍼레이션과 적용에 대해 기술한 표준이다. 본 표준에서 기술하

이 논문은 2008년 호원대학교 교내연구비의 지원에 의하여 연구되었음.
[1]호원대학교 컴퓨터학부
*교신저자: 이기성(ygslee@howon.ac.kr)

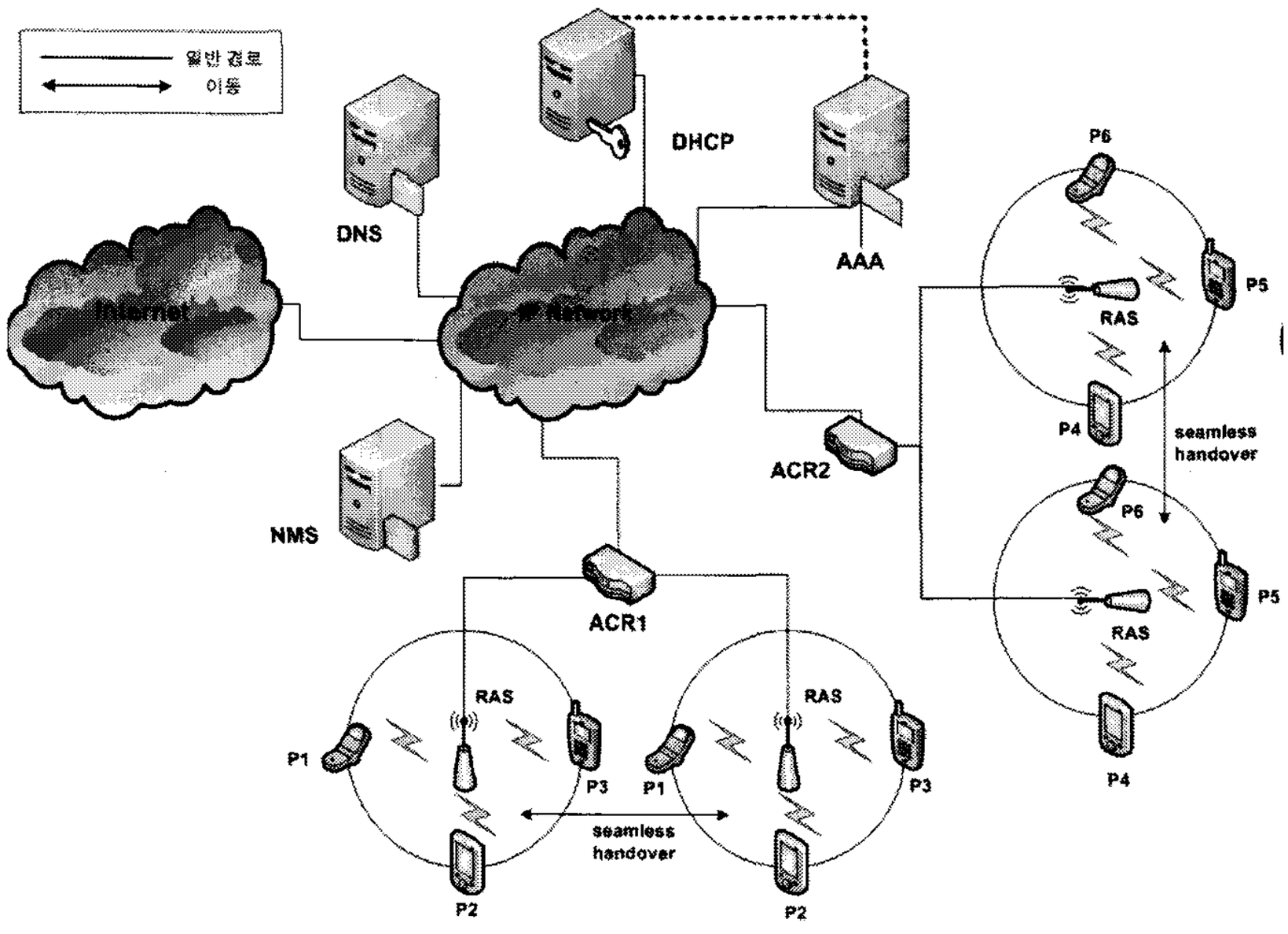
는 세부 항목은 다음과 같다. 네트워크 참조 모델, 적용 시나리오, 와이브로 네트워크 상에서의 IPv6 패킷 전달, 이웃 탐색 프로토콜, 상태 보존 및 상태 비 보존 주소 자동설정, 멀티캐스팅, 이동성, 보안 등이다. 와이브로는 이동하면서 광대역 인터넷 서비스를 가능하게 한다. IPv6는 광대역 IP 주소 영역을 제공함과 동시에 이동성을 효율적으로 제공할 수 있다. 그러므로 와이브로에서의 IPv6 표준은 차세대 All-IP 서비스를 위한 핵심기술로 활용될 것이다[2]. 다음으로, "휴대인터넷(와이브로 TM) 서비스를 위한 상호 인증 절차[3]"는 PISIM(Portable Internet Subscriber Identity Module : 휴대인터넷(와이브로 TM) 가입자 인증 모듈) 기반의 사용자와 망간의 상호 인증 방식을 정의하고 이 과정에서 요구되는 PE(Portable Equipment: 단말기)와 PISIM 사이의 인터페이서에 대한 표준을 정의한다. 상호 인증 절차 부분에서는 PISIM과 PE, PE와 RAS(Radio Access Station: 기지국) 또는 ACR(Access Control Router: 제어국), RAS 또는 ACR과 AS(Authentication Server: 인증 서버)간의 메시지 구조와 전달 파라미터, PISIM, PE, RAS 또는 ACR, AS의 역할을 구체적으로 정의하며, PE와 PISIM 간의 인터페이스 부분에서는 PE와 PISIM 간의 초기화 과정, PE와 PISIM 사이의 인증 메시지 전달 방식, 그리고 네트워크 정보와 인증 및 사용자 정보를 저장하는 PISIM 내의 파일 등을 정의한다. 이 방식에서 인증 시그널링은 RFC 3748에 명시된 EAP(Extensible Authentication Protocol) 방식에 기반하고, 휴대인터넷(와이브로 TM)과 이종 망간의 연동을 고려하기 위해 통합 인증에 적합한 EAP-AKE(Authentication Key Agreement) 방식을 이용한다. 인증 절차에 대한 구체적인 내용은 다음절에서 기술하기로 한다.

이 방식은 핵심은 PE에서 인증하는 것이 아니라 PISIM에서 AKA 절차를 수행하며, 사용자의 비밀 정보 및 키 값을 저장, 관리한다. 단지 PE는 PISIM 탈/부착이 가능한 단말 또는 PISIM 기능을 hand-wired logic 형태로 제공하는 machine-to-machine 형태의 단말에 국한하고 있다. 이 표준 프로토콜의 문제점은 PISIM 카드의 분실이나 에러가 발생했을 경우에 ACR은 단말을 인증할 수 없기 때문에 사용자는 원활한 무선인터넷 서비스를 받을 수 없게 된다. 또한 인증 절차에 필요한 메시지의 수가 대체로 많은 편이다.

따라서 본 논문에서는 PISIM 대신에 PSD(Portable Support Device)가 PSS와 ACR 간에 키 동의에 참여하게 된다. 인증키를 생성한 후에는 ACR과 안전한 통신 세션을 맺고 있는 KAS(Key Authentication Server)에 PSS 식별자와 키를 암호화해서 저장한다. PSS가 다른 네트워크로 이동하여 무선인터넷에 재접속을 해야 할 경우에는 인증키로 암호화한 재접속 요청 메시지를 새로운ACR은 수신한 후에 KAS로 그 메시지를 전송하면 KAS는 PSS를 인증한 후에 새로운 ACR에게 인증키를 전송한다. 인증키를 통해 새로운 ACR은 PSS로부터 수신한 메시지를 확인한 후에 접속을 허가한다. 이 논문의 구성은 다음과 같다. 2장에서는 본 연구를 위한 연구배경에 대해서 살펴보고, 3장에서는 제안하는 프로토콜에 대해 자세히 기술한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 끝으로 5장에서는 결론과 향후 연구방향을 제시한다.

2. 서론

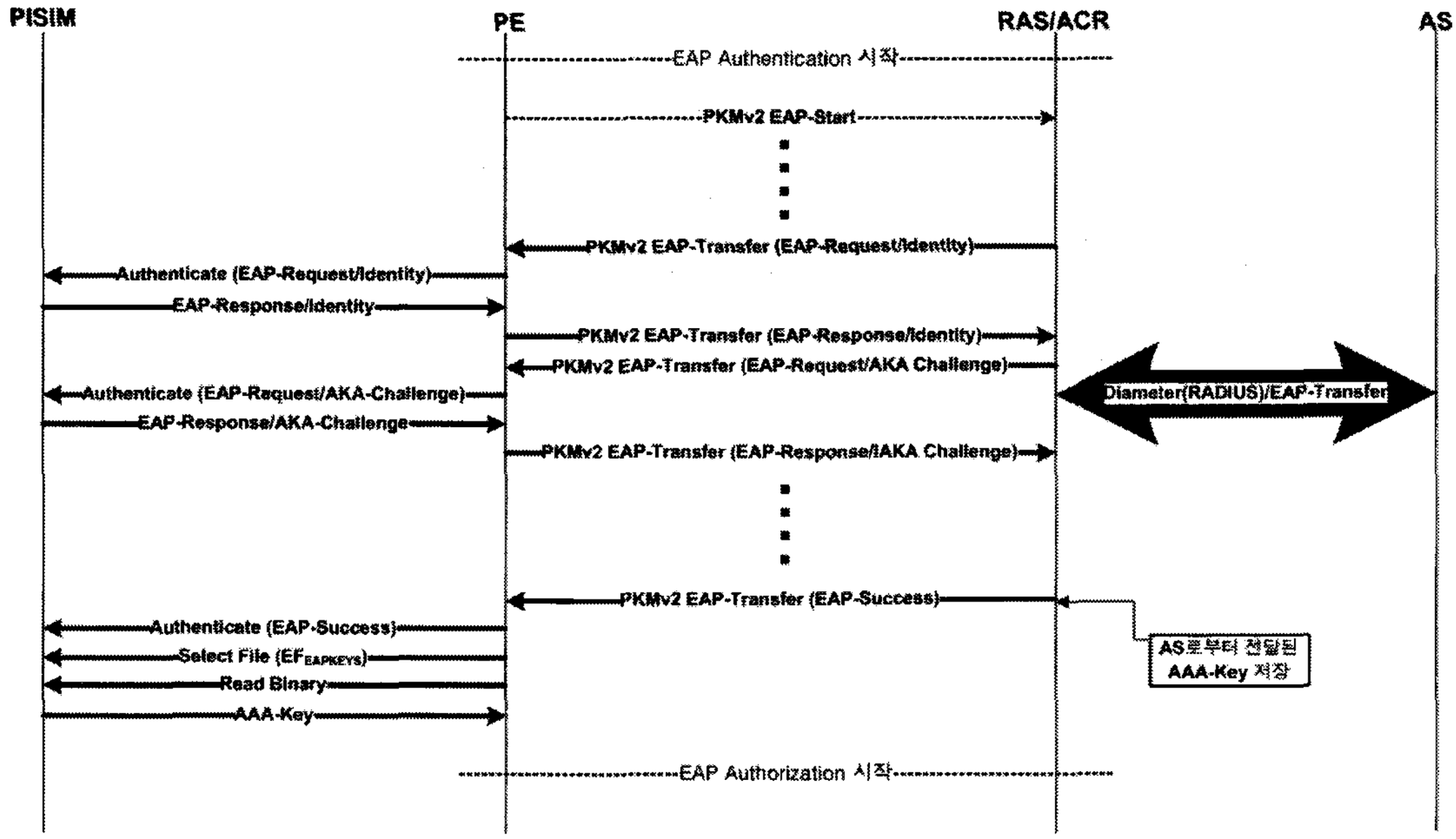
한국정보통신기술협회(TTA)에서는 와이브로에서의 IPv6 기술[2]과 휴대인터넷(와이브로 TM) 서비스를 위한 상호 인증 절차[3]에 대한 표준을 제정했다. [2]는 와이브로 네트워크 상에서의 IPv6 오퍼레이션과 적용에 대한 사항들을 기술하고 있다. 본 표준에서 기술하는 세부항목은 네트워크 참조 모델, 적용 시나리오, 와이브로 네트워크 상에서의 IPv6 패킷 전달, 이웃 탐색 프로토콜을 포함한 이동성, 보안 등에 기반하고 있다. 와이브로 서비스를 위한 네트워크 구조는 그림 1과 같다. P1-P6는 PSS(Portable Subscriber Station)으로서 실제 사용자 또는 가입자와 BS(Base Station) 간에 연결을 제공하며 무선인터넷 서비스를 받기 위해 사용하는 PDA, 핸드폰, 노트북과 같은 일반화된 이동장비이다. RAS(Radio Access Station)은 PSS와 ACR(Access Control Router) 간에 연결을 제공하는 장비로서 WiMAX에서는 BS로도 정의된다. ACR은 RAS와 IP 네트워크 간에 연결을 제공하며 PSS에 있어서 최초의 홉 라우터로써의 기능을 수행한다. 또한 ACR은 NAC(Network Access Control), AAA(Authentication, Authorization, Accounting), 주소 할당 및 등록, 연결에 대한 파라미터 변경과 같은 접속 제어 기능을 제공해야 한다. NMS(Network Management System)은 네트워크를 관리 시스템이며 DHCP는 AAA(Authentication, Authorization, Accounting) 서버와 연결되어 있는 구조를 가진다. IPv6는 Dual-stack에 PSS, RAS과 ACR 장비를 업그레이드 해서 전개된다. RAS는 Layer 2의 기능을 제공하는 브릿지 모드로 동작한다. 따라서 IPv6 서비스를 제공하기 위해 어떠한 변화도 필요 없게 된다. RAS와 ACR 간은 유선 네트워크로 구성할 수도 있다. RAS가 layer 2의 기능을 제공하기 때문에 PSS가 ACR 내부에서는 핸드오버가 발생해도 끊김없는 무선인터넷 서비스를 제공받을 수 있다. 하지만 PSS가 ACR1에서 ACR2로 이동할 경우에는



[그림 1] 와이브로에서 IPv6 서비스를 제공하기 위한 네트워크 구조의 예

MIPv6에 기반한 핸드오버 처리를 수행해야 할지도 모른다. 무엇보다도 PSS가 무선인터넷 서비스를 제공받기 전에 PAS 또는 ACR에서는 PSS를 인증해야 할 것이다.

PSS와 PAS 또는 ACR 간에 인증 서비스를 제공하기 위해 TTA에서는 휴대인터넷(와이브로 TM) 서비스를 위한 상호 인증 절차[3]를 표준으로 채택했다. 이 표준은 PISIM(Portable Internet Subscriber Identity Module: 휴대인터넷(와이브로 TM) 가입자 모듈) 기반의 사용자와 망 간의 상호 인증 방식을 정의하고 이 과정에서 요구되는 PE(Portable Equipment)와 PISIM 사이의 인터페이스에 대한 표준을 정의한다. [그림 2]는 PISIM을 이용한 PE와 RAS 또는 ACR간에 상호 인증 과정을 보여준다. 먼저 링크가 활성화된 후, PE에서 PKM(Privacy Key Management)v2 EAP(Extensible Authentication Protocol) -Start 메시지를 RAS/ACR에게 전송하여 인증을 시작하거나 RAS/ACR에서 PKMv2 EAP-Transfer(EAP-Request /Identity) 또는 PKMv2-Transfer(EAP-Request/AKA-Identity) 메시지를 PE에게 전송하여 인증을 시작한다. 그런 다음 RAS/ACR은 사용자의 identity를 요구하는 EAP-Request/Identity 또는 EAP-Request/AKA(Authentication Key Agreement)-Identity 메시지를 PE에게 전송한다. 이 메시지는 MAC 관리 메시지 중 PKMv2 EAP-Transfer 메시지에 캡슐화되어 전송되며 이 캡슐화는 모든 EAP-AKA 메시지에 동일하게 적용된다. PE는 이 PKMv2 EAP-Transfer 메시지를 해석하여 EAP-Request/Identity 또는 EAP-Request/AKA-Identity 메시지를 추출한 뒤 PISIM이 이해할 수 있도록 EAP-Request/Identity 또는 EAP-Request/AKA-Identity 메시지를 APDU (Application Protocol Data Unit) 형태로 변환하여 전달한다. EAP-Request/Identity 또는 EAP-Request/AKA-Identity 메시지를 수신한 PISIM은 사용자 identity를 EAP-Response/Identity 또는 EAP-Response/AKA-Identity 메시지를 통해 PE로 전송하며, 이 메시지는 PE에서 PKMv2 EAP-Transfer 메시지에 캡슐화되어 RAS/ACR로 전송된다. RAS/ACR은 PE로부터 전달된 PKMv2 EAP-Transfer 메시지를 해석하여 EAP-Response/Identity 또는 EAP-Response/AKA-Identity 메시지를 AS에게 전달하며, 이 때 RAS/ACR과 AS간에 Diameter 또는 RADIUS 프로토콜을 통해 메시지를 송수신한다. 즉, Diameter(RADIUS)/EAP-Transfer 메시지에 EAP-Response/Identity 또는 EAP-Response/AKA-Identity 메시지가 캡슐화되어 전송되고, 이 캡슐화는 모든 EAP-AKA 메시지에 동일하게 적용된다. AS는 EAP-Request/AKA-Challenge를 Diameter(RADIUS) /EAP-Transfer 메시지에 캡슐화하여 RAS/ACR에게 전송하고 RAS/ACR은 수신된 메시지를 해석하여 PKMv2 EAP-Transfer 메시지로 변환한 뒤 PE에게 전송한다. PE는 이 PKMv2 EAP-Transfer 메시지를 해석하여 EAP-Request/AKA-Challenge를 APDU 형태로 변환하여 PISIM에게 전달한다. PISIM은 EAP-Request/AKA-Challenge



[그림 2] PISIM을 이용한 휴대인터넷(와이브로 ™) 상호 인증

메시지에 포함된 여러 파라미터를 이용하여 AKA 알고리즘을 통해 네트워크 인증을 수행하고 EAP-AKA 인증 프로토콜 수행에 필요한 여러 가지 키 값들을 생성하여 관련 파일에 저장한다. PISIM은 수행이 성공적으로 완료된 후, 인증 파라미터를 EAP-Response/AKA-Challenge를 통해 PE로 전송하며, 이 메시지는 PE에서 PKMv2 EAP-Transfer 메시지에 캡슐화되어 RAS/ACR로 전송된다. RAS/ACR은 이 PKMv2 EAP-Transfer 메시지를 해석하여 EAP-Response/AKA-Challenge를 Diameter(RADIUS) /EAP-Transfer 메시지에 캡슐화하여 AS로 전달한다. 인증 절차가 성공적으로 수행된 후, AS는 EAP-Success 메시지를 Diameter(RADIUS)/EAP-Trasnfer 메시지에 캡슐화하여 RAS/ACR에게 전송하고 RAS/ACR은 다시 이 메시지를 해석하여 PKMv2 EAP-Transfer 메시지로 변환한 뒤 PE에게 전송한다. 이 때 AS는 Diameter(RADIUS) /EAP-Transfer 메시지의 AVP에 AAA-Key(MSK)를 포함시켜 RAS 또는 ACR에게 전달하고 RAS/ACR은 수신한 AAA-Key(MSK)를 안전하게 저장한다. PE는 이 PKMv2 EAP-Transfer 메시지로부터 획득한 EAP-Success 메시지를 APDU 형태로 변환한 뒤 PISIM에게 전달하며 PISIM은EAP-Success 메시지를 통해 인증 과정이 성공적으로 끝났음을 확인한다. 이후 PE는 PKMv2 키 유도 방법을 이용하여 휴대인터넷(와이브로 TM) 키 값들을 생성하기 위해 필요한 AAA-Key(MSK)를 $EF_{EAPKEYS}$ 파일로부터 읽어온다. 하지만 이 표준 방식은 PE가 무선인터넷 서비스를 받기 전에 RAS/ACR과 인증을 시도한 후에 인증이 완료되면 서비스를 받는 방식이다. 이 때, PISIM은 PE의 인증모듈로서 PE가 무선인터넷에 접속하기 위해서 RAS/ACR 간에 인증을 돕는 역할을 수행한다. 하지만 이 표준 방식에서 PISIM이 차지 하고 있는 비중은 매우 높다. PISIM을 분실하거나 애러가 발생했을 경우에는 PE가 외부 ACR로 이동했을 경우에 무선인터넷 서비스를 받지 못할 수 있다. 또한 인증 절차에 필요한 메시지의 수가 대체로 많은 편이다.

3. 제안하는 프로토콜

본 절에서는 PSS와 ACR 간의 키 동의 프로토콜을 제안한다. 제안하는 프로토콜에서 ACR과 KAS는 안전한 IPsec 터널을 통해 데이터를 주고받는다. PSD는 PSS에 대한 계산량을 지원하기 위한 장치로서 키 동의 프로토콜이 끝난 후에는 사용을 하지 않으며 USB와 같은 데이터 저장 공간으로 재사용할 수 있다. 또한 PSD가 분실되었을 경우에도 PSS가 추가 키 동의 프로토콜을 수행하지 않고 기존에 생성한 키를 가지고 외부 링크의 ACR과 접속을 위한 인증 절차를 수행할 수 있다. 본 프로토콜에서 RAS는 PSS로부터 전송된 메시지를 ACR에게 포워딩하는 AP(Access point) 역할만 수행한다.

3.1 표기법

[표 1] 표기법

표기	의미
PSS	Portable Subscriber Station
RAS	Radio Access Station
ACR	Access Control Router
PSD	Power Support Device
KAS	Key Authentication Server
ID_X	X에 대한 식별자 or 주소
prf(k,m)	키 k와 메시지 m을 입력으로 하는 pseudo random function
sig^X	노드 X의 서명
g^X	노드 X의 Diffie-Hellman 키동의에 필요한 파라미터
h(m)	메시지 m을 입력으로 하는 MDC 해시 함수
$+k^X/-k^X$	노드 X의 공개키/개인키
k^{DH}	Diffie Hellman 세션키
k^{AU}	PSS와 ACR 간의 인증키
$Cookie^I$	서비스 거부 공격과 경로변경 공격을 완화하기 위한 I번째 쿠키
n^IX	노드 X의 I번재 nonce
NAI^{IX}	노드 X의 I번째 network access identifier
L^X	노드 X의 Lifetime
m1‖m2	메시지 m1과 메시지 m2의 비트 결합

3.2 키 동의 프로토콜

키 동의 프로토콜은 그림 3과 같다. 먼저 PSS1은 무선 인터넷 접속을 위해 RAS1을 거쳐 ACR1에게 다음과 같은 인증 요청 메시지를 전송한다.

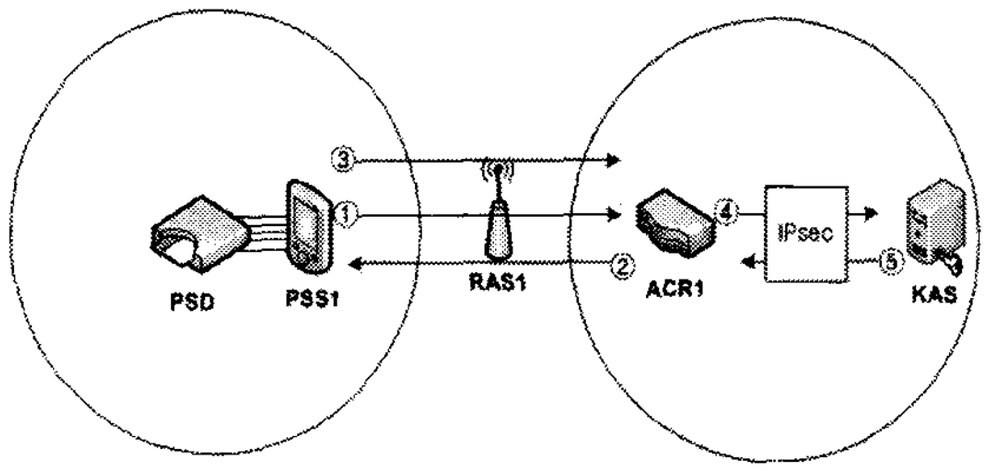
①

$$PSS1 \rightarrow ACR1\,(REQ) : ID_{PSS1}, NAI^1_{PSS1}, g^x, N^1_{PSS1}, L_{PSS1}, Cookie^1_{PSS1}, Sig(-K_{PSS1}, h(ID_{PSS1} \| NAI^1_{PSS1} \| g^x \| N^1_{PSS1} \| L_{PSS1} \| Cookie^1_{PSS1}))$$

PSS1은 네트워크 접속 식별자인 NAI[4]를 인증 요청 메시지에 추가하며 서명을 포함한 공개키 연산은 PSD에서 지원해준다. $Cookie^1_{PSS1}$[5]는 도스 공격과 경로 변경 공격을 완화하기 위해 추가된 파라미터이며 서명은 Diffie-Hellman 키동의 프로토콜에서 발생할 수 있는 중간자 공격을 방지하기 위해 사용된다. 이 메시지를 수신한 ACR1은 네트워크 접속 식별자를 확인하고 PSS1의 공개키를 이용하여 서명을 확인한다. 그런 후에 다음과 같은 응답 메시지를 전송한다.

②

$$ACR1 \rightarrow PSS1\,(REP) : ID_{ACR1}, g^y, N^1_{ACR1}, N^1_{PSS1}, L_{ACR1}, Cookie^2_{ACR1}, Sig(-K_{ACR1}, h(ID_{ACR1} \| g^y \| N^1_{PSS1} \| N^1_{ACR1} \| L_{ACR1} \| Cookie^2_{ACR1}))$$



[그림 3] PSS1과 ACR1 사이의 키동의 프로토콜

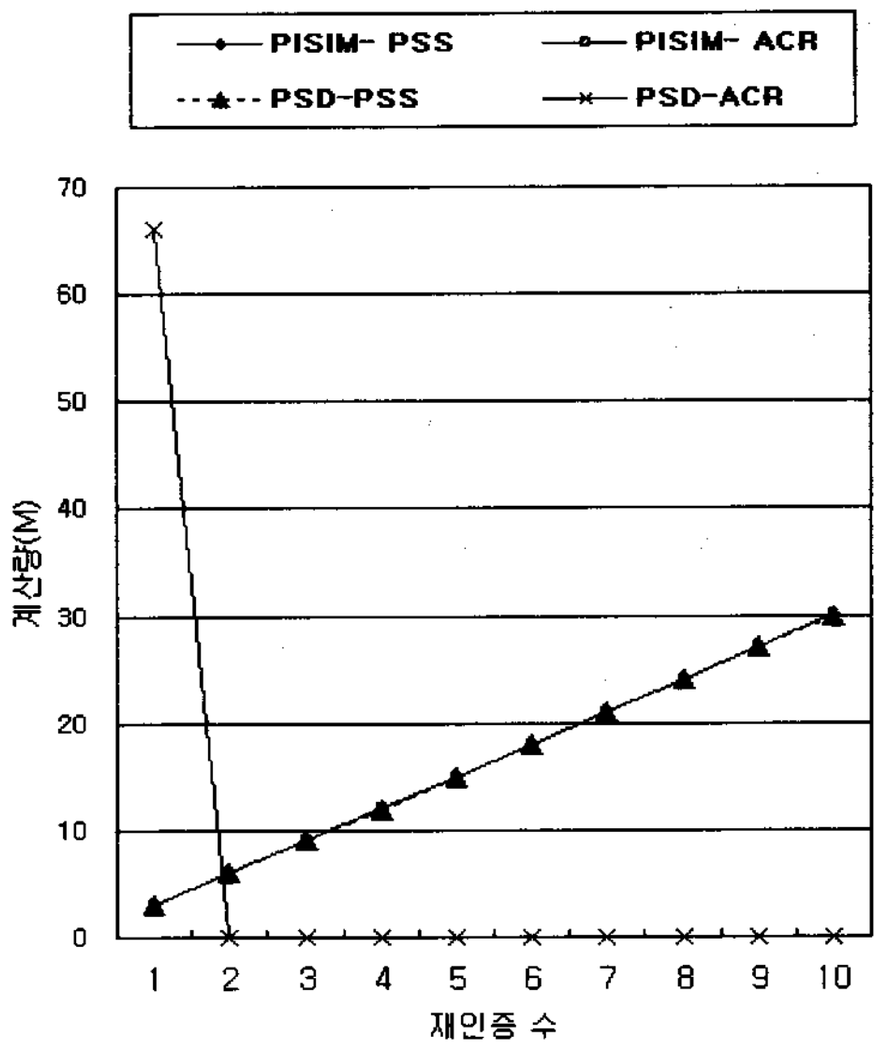
ACR1은 Diffie-Hellman 키 동의 파라미터 g^y 를 생성하여 응답 메시지에 추가하고 자신의 개인키로 서명하여 PSS1에게 전송한다. ACR1은 PSS1로부터 수신한 g^x와 자신이 생성한 g^y를 이용하여 Diffie-Hellman 키 $K^{DH}=g^{xy}$를 생성한다. PSS1 역시 PSD의 계산력을 이용하여 ACR1과 같이 $K^{DH}=g^{xy}$를 생성한다. 그런 후에 최종적으로 PSS1과 ACR1은 $K^{AU}=prf(K^{DH}, Cookie^1_{PSS1} \| Cookie^2_{PSS2})$를 생성한다. ACR1은 생성된 인증키를 KAS에게 PSS1 식별자와 함께 안전한 IPsec 터널을 통해 KAS에게 전송한다. 이때 PSS1은 생성된 인증키를 이용해서 무선 인터넷 접속 메시지③을 ACR1에게 전송하면 ACR1은 인증키로 메시지를 인증한 후에 PSS1의 무선인터넷 접속을 허가한다. 그런 후에 ACR1은 인증키를 IPsec 터널을 통해 KAS에게 PSS1의 식별자와 인증키를 포함한 메시지④를 전송한다. KAS는 수신한 PSS1의 식별자와 인증키를 암호화 한 후에 저장하고 확인 메시지⑤를 ACR1에게 전송한다. PSS1가 ACR1의 서비스 지역에 있다가 다른 네트워크 ACR2로 이동하면 더 이상 ACR1의 서비스를 받지 못하기 때문에 PSS1은 접속 요청 메시지를 ACR2에게 전송한다. 이때 ACR2는 KAS에게 이 메시지를 넘겨주고 KAS는 이 메시지를 인증하여 ACR2에게 PSS1의 인증키를 전송한다. 이 키를 통해 ACR2는 PSS1을 인증하고 접속을 허가한다.

4. 성능분석

이번 절에서는 앞서 제안한 키 동의 프로토콜의 안전성과 효율성을 표준 프로토콜과 비교 분석할 것이다. 비교 분석은 표 2와 같다. 먼저 표준 프로토콜[3]과 제안하는 프로토콜의 안전성을 분석해보면 두 프로토콜 역시 DoS 공격, 경로 변경 공격 및 중간자 공격에는 안전하다는 것을 볼 수 있다. 특히, 제안하는 프로토콜에서는 쿠키를 이용해서 올바르지 않은 메시지일 경우에는 바로 수신한 메시지를 드롭하기 때문에 경로 변경 공격이나 DoS 공격을 완화할 수 있다. 또한 Diffie-Hellman 키 동의시 발생할 수 있는 중간자 공격은 서명을 통해 방지할 수 있다. 효율성 분석은 ETBU(Extended Ticket-Based Binding Update)[6] 프로토콜을 이용한다. 제안하는 프로토콜의 경우 저전력 노드일 수 있는 PSS의 계산적 부담을 PSD에서 처리하기 때문에 실질적으로 PSS는 적은 계산량으로 키동의를 할 수 있다. ACR은 PSS보다 전력이나 계산량에 제한을 받지 않기 때문에 대체적으로 계산량이 많지만 별 무리가 없다. 또한 표준 프로토콜[3]보다 적은 양의 메시지와 간단한 방법으로 인증을 할 수 있다.

[표 2] 프로토콜의 안전성과 효율성

분석요소				[3]	제안하는 프로토콜
DoS 공격				○	○
경로 변경 공격				○	○
중간자 공격				○	○
재생 공격				○	○
메시지 수				최소 14 이상	5
PSS	RSA	암호화		1*3028K	1*3028K
		DS (RSA -PSS)	서명	0	0
			검증	0	0
	MAC/prf			6*0.026K	1*0.026K
	합계			≈3028.156K	3028.026K
ACR	RSA	암호화		1*3028K	1*3028K
		DS (RSA -PSS)	서명	0	1*62000K
			검증	0	1*3019K
	MAC/prf			6*0.026K	1*0.026K
	합계			≈3028.156K	68047.026K



[그림 4] PISIM 기반 프로토콜[3]과 제안하는 PSD 기반 프로토콜의 효율성 분석

또한 PSS가 재접속을 요구할 경우에는 KAS로부터 인증만 받으면 되기 때문에 PISIM 기반 프로토콜[3] 보다 더욱 간단한 방법으로 인증할 수 있다. 또한 그림 4에서 노드간 재인증 수가 증가할 경우 PISIM 기반 프로토콜은 계산량이 정비례하는 반면에 제안하는 PSD 기반의 프로토콜은 PSD-ACR의 경우 반비례하다가 0.0026M로 일정하다는 것을 볼 수 있다. 휴대 인터넷의 경우 이동하면서 핸드오프가 빈번하게 일어나는 것을 고려하면 재인증 수는 증가할 수밖에 없다.

5. 결론

본 논문은 안전한 WiBro 서비스를 위한 새로운 인증 프로토콜에 대해서 제안했다. 제안하는 프로토콜 역시 표준 프로토콜[3]과 안전성 면에서는 큰 차이를 보이지 않았다. 그러나 효율성 분석에서는 적은 양의 메시지 사용과 재접속 시에 간단한 방법으로 인증이 가능하다.

참고문헌

[1] 이광희, "와이브로 기술의 국제표준채택에 따른 향후 전망", Korea Telecommunications Operators Association, 제 49호, 2007.

[2] 김홍구, "와이브로에서의 IPv6 기술(IPv6 over

WiBro)", 한국정보통신기술협회, 2006.
[3] 김홍구, "휴대인터넷(와이브로 TM) 서비스를 위한 상호 인증 절차", 한국정보통신협회, 2006.
[4] A. Patel, K. Leng, H. Akhtar, M. Khalil, "Network Access Identifier Option for Mobile IPv6," IETF Internet Draft, July 2004.
[5] P. Kern and W. Simson, "Photuris: Extended Schemes and Attributes", RFC 2523, March 1999.
[6] Jung-Doo Koo and Dong-Chun Lee, "Extended Ticket-Based Binding Update (ETBU) Protocol for Mobile IPv6 (MIPv6) Networks, IEICE Transactions on Communications, vol.E90-B, no.4, pp.777-787, April 2007.

이 기 성(Gi-Sung Lee) **[종신회원]**

- 1993년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

<관심분야>
이동통신, 멀티미디어 통신, 네트워크 보안