전방향 안정성을 제공하는 Wibro인증 및 키 동의 프로토콜

이승우, 박희주, 이진호
경일대학교 컴퓨터공학부
e-mail: hjpark@kiu.ac.kr

Wibro Authentication and Key Agreement Protocol providing Forward Secrecy

Seung-Woo Lee, Hee-Ju Park, Jin-Ho Lee
School of Computer Engineering, Kyungil University

요 약

언제 어디서나 인터넷에 접속하여 필요한 정보를 얻을 수 있는 서비스를 Wibro(Wireless Broadband)라고 한다. 서비스를 제공하기 위해 중요한 기술요소 중 하나가 보안이다. 최근 보다 안전한인증 메커니즘을 설계할 수 있는 UICC기반의 EAP-AKA프로토콜이 제안되었다. 그러나 이 프로토콜은 프라이버시 보호 문제와, 인증서버에 저장공간 오버헤드, 비밀키 노출에 따른 전방향 안전성제공의 문제점들이 있다. 본 논문에서는 UICC기반의 EAP-AKA프로토콜의 문제점을 살펴보고 이러한 문제점을 해결하기 위한 전방향 안정성을 제공하는 Wibro인증 및 키 동의 프로토콜을 제안한다.

1. 서론

언제 어디서나 인터넷에 접속하여 필요한 정보를 얻을 수 있는 서비스를 Wibro(Wireless Broadband)라고 한다[2]. 이러한 Wibro의 안전한 서비스를 제공하기 위해 중요한 기술요소 중 하나가 보안이다. 특히 Wibro단말 사이의 무선 링크상에서 사용되어지는 모든 키들을 안전하게 생성하고 공유하기 위해 정의하는 보안키 관리(PKM : Privacy Key Management)가 중요하다.

현재 Wibro시스템에서는 크게 두개의 PKMv1과 PKMv2의 프로토콜이 존재한다[3]. 현재 Wibro은 PKMv1 보다 비도가 높은 PKMv2이 사용된다. 최근 3GPP에서 PKMv2 프로토콜 기반의 무선랜과의 연동을 위해 제안한 인증 프로토콜인 EAP-AKA를 Wibro에 적용하여 사용자와 네트워크간의 상호인증 및 사용자 인증정보를 UICC기반의 스마트가트에서 관리 및 처리함으로 보다 안전한 인증 메커니즘을 설계할 수 있는 UICC기반의 EAP-AKA 프로토콜이 제안되었다[4],[5],[7].

그러나 UICC기반의 EAP-AKA프로토콜은 사용자의 유일한 ID의 평문상태전송으로 인한 노출 발생으로 인해 발생할 수 있는 프라이버시 보호 문제와 다수의 *AV*를 사용함으로써 인증서버(AAA)의 저장공간 오버헤드 발생문제 또한 전방향 안전성을 제공하지 못하는 문제가 있다.

본 논문에서는 제안된 UICC기반의 EAP-AKA프로토콜의 문제점을 해결하고 전방향 안전성을 제공하는 새로운 UICC기반의 EAP-AKA프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 Wibro네트워크의 전체적인 구성과 구성요소에 대해 살펴보고, 기존에 제시된 UICC기반의 EAP-AKA프로토콜의 구성과 구성요소 및 인증절차에 대해 알아본 후 문제점을 분석한다. 3장에서는 제안하는 프로토콜에 대해 설명하고, 4장에서는 프로토콜의 안정성 분석을 한다. 5장에서는 결론을 맺는다.

2. 연구배경

본 장에서는 Wibro네트워크에 구성과 구성요소를 살펴보고 UICC기반의 EAP-AKA프로토콜의 구성요소 그리고 진행과정을 살펴본다. 마지막으로 UICC기반의 EAP-AKA 프로토콜에 문제점을 분석한다.

2.1 휴대인터넷(WiBro) 네트워크

이들 구성요소에 대한 설명은 다음과 같다[6].

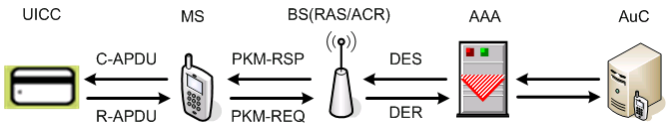
- ◈ PSS(Portable Subscriber Station) : 가입자가 휴대인넷 서비스를 제공받기 위한 휴대인터넷용 무선단말기를 말한다.
- ◈ RAS(Radio Access Station) : 유선 네트워크 종단에서 무선 인터페이스를 통해 단말과 송수신을 하는 구성 요소이다.
- ◈ ACR(Access Control Router) : 단말과 기지국을 제어하고, IP패킷을 라우팅하는 구성 요소이다.
- ◈ AAA(Authentication, Authorization, Accounting) : 적법한 사용자에 한해 휴대인터넷 망에 접속, 서비스를 제공하기 위해 사용자 및 단말에 대한 인증 권한

검증 및 과금을 수행하는 구성 요소이다.

◈ HA(Home Agent) : 홈 네트워크에서 단말의 IP이동성을 지원하는 망 구성 요소이다.

2.2 UICC기반의 EAP-AKA프로토콜

본 소절에서는 UICC기반의 EAP-AKA프로토콜[4] 의 구성요소를 살펴본 후 UICC기반의 EAP-AKA프로토콜의 인증 절차에 대해 기술한다.



(그림 2) UICC기반의 EAP-AKA를 위한 네트워크 구성

◈ AuC(Authentication Center) : 인증 데이터 센터로서 3GPP에서는 별도의 AuC가 구성된다. 3GPP-WLAN과의 연동을 고려한 경우는 연동 보안을 관리하는 AuC가 *AV*(Authentication Vector)를 생성한다. Wibro무선 네트워크 인증 메커니즘만을 고려할 경우 AuC의 역할을 AAA인증서버가 할 수 있다.[6]

◈ UICC(Universal IC Card) : WIBRO 단말에서 Wibro 망에 접속시 UICC를 이용하여 안전하게 가입자 인증을 수행한다.

◈ Terminal(단말 MS) : 휴대용 단말에 해당하는 무선 장비를 말한다.

◈ BS(Authenticator) : 무선국과 통신하기 위한 고정 무선국을 말한다.

◈ EAP Server/(AAA인증 서버) : "인증(Authentication), 권한검증(Authorization), 계정관리(Accounting)"의 구현 및 분산 보안을 위한 인증용 프로토콜 또는 서비스를 말한다.

임선희 등이 제안한 UICC기반의 EAP-AKA프로토콜은 초기 등록 과정을 거쳐 인증 절차에 필요한 초기값을 UICC와 AuC간에 공유한다. 이후 인증 시나리오가 다음과 같이 진행된다[5]. UICC기반의 EAP-AKA프로토콜의 진행 과정을 살펴보면 우선 MS가 BS에게 인증시작을 요청하면 BS는 사용자ID를 요청한다. MS는 UICC에게 사용자ID를 요구하고 UICC는 사용자의 유일한 아이디를 평문형태로 AuC에게 전송한다. UICC로부터 사용자ID를 전달받은 AuC는 테이터베이스에서 해당 ID를 검색한다. AuC는 *AV*를 생성하고 AAA인증서버에게 전달한다. AAA는 전달받은 *AV*값 중 *AT_RAND, AT_AUTN, AT_MAC* 을 BS와 MS를 거쳐 UICC에게 전달한다. 값을 수신한 UICC는 *AUTN*의 *MAC*값과 계산한 *XMAC*값을 비교하여 검증한다. 검증이 이루어진 후 UICC는 *RES*를 계산하여 AAA로 보낸다. 수신한 AAA는 자신이 계산한 *XRES*와 비교하여 검증한다. 검증이 성공하면 상호인증이 이루진다. 이후 UICC와 AAA는 *MS*(Master Key)를 이용해 통신에 사용할 키들을 생성한다.

2.3 UICC기반의 EAP-AKA프로토콜의 문제점 분석

본 소절에서는 기존 UICC기반의 EAP-AKA프로토콜의 프라이버시 보호 문제와 인증서버의 저장공간 오버헤드 문제 그리고 전방향성 제공에 대한 문제점에 대해 분석한다.

◈ 프라이버시 보호 문제
MS가 새로운 BS에 방문할 경우 적어도 한번은 사용자의 유일한 ID를 평문형태로 전송할 때 발생할 수 있는 프라이버시 보호에 대한 문제점이 있다.

◈ 인증서버의 저장공간 오버헤드 문제
AuC의 다수의 *AV*생성과 AAA에 전달하는 과정에서 발생할 수 있는 AAA의 저장공간 오버헤드와 대역폭 소모 문제점있다.

◈ 전방향성 제공 문제
비밀키 *K*가 장시간 노출 되었을 때 이전 세션키를 얻을 가능성이 있다. 제안하는 프로토콜에서는 세션키 생성시 *TK*를 이용하여 생성함으로써 이를 해결한다.

3. 새로운 UICC기반의 EAP-AKA프로토콜

본 장에서는 제안하는 프로토콜의 가정과 표기법에 대해 살펴본 후 기존 UICC기반의 EAP-AKA프로토콜의 문제점을 해결하기 위한 새로운 프로토콜을 제안한다.

3.1 제안하는 프로토콜의 가정

제안하는 프로토콜은 다음과 같은 가정을 가진다. MS와 HN은 비밀키 *K*와 임시 ID인 TID_{MS} 그리고 암호 알고리즘을 공유하고 있고 BS과 AAA는 IPsec이나 MACsec과 같은 네트워크 도메인 보안 메커니즘을 통해 안전한 통신을 한다고 가정한다. 그리고 AuC의 역할을 AAA 인증서버가 한다고 가정한다.

3.2 표기법

본 논문에서 사용하는 표기법은 (표 1)과 같다.

3.3 프로토콜

본 소절에서는 제안하는 프로토콜에 대해 설명한다. 제안하는 프로토콜은 임시 ID를 사용하여 프라이버시 보호를 제공하고 티켓 기반의 인증을 수행하여 *AV*사용의 문제점을 해결하였다 또한 티켓키기반의 세션키를 생성함으로써 전방향 안전성을 제공한다. (그림 3)는 제안하는 프로토콜의 전체적인 수행 과정을 보여준다.

Step 0 : MS는 BS에게 PKM요청메시지로 *PKMv2 EAP Start* 메시지를 보내어 인증 시작을 요청한다. *PKMv2 EAP Start* 메시지를 수신한 BS는 EA-

(표 1) 프로토콜 표기법

기호	설명
K	AuC와 공유하는 비밀키
N_A	A에서 생성한 난수
TDI	프라이버시 보호를 위해 사용되는 임시 ID
$f_K^1()$	MAC(Message Authentication Code)값을 계산하는 메시지 인증함수
$f_K^2()$	RES or $XRES$ 값을 계산하는 메시지 인증 함수
$f_K^3(),f_K^4(),f_K^5()$	각각의 키를 생성하는 함수
g	$g<p$이고, p와 서로소인 원시근
p	매우 큰 소수
$XMAC_A$	A가 생성한 메기지 인증 코드 값에 대응 하는 값
AMF	다중 인증 알고리즘과 키를 지원하거나 암호화키와 무결성키의 수명을 관리하는 인증 관리 필드(Authentication Management Field)
TK	제안하는 프로토콜에서 사용되는 티켓 키
CK	$f_K^3()$함수에 의해 생성되는 암호화 키
IK	$f_K^4()$함수에 의해 생성되는 암호화 키
RES_A or $XRES_A$	A가 $f_K^2()$함수로 생성하는 인증 응답 값과 그에 대응하는 기대 값

P인증 절차를 시작하고 인증 서버와 연결하여 EAP 프로토콜의 중계 역할을 한다.

(MS ⇒ BS)

PKM-REQ[*PKMv2 EAP Start*]

Step 1 : MS로부터 *PKMv2 EAP Start* 메시지를 수신한 BS는 MS에게 ID 요청메시지를 보낸다. BS로부터ID요청메시지를수신한MS는 UICC카드로 사용자신원 요구메시지를 EAP 패킷으로 보낸다.

(BS ⇒ MS)

PKM-RSP[*EAP Request/Identity*]

(MS ⇒ UICC)

EAP Request/Identity

Step 2 : 사용자 신원 요구 메시지를 수신한 UICC는 랜덤값 $a \in Z_p$를 선택하고 A와 타임스탬프 T_{UICC} 그리고$MAC_{UICC} = f_K^1(A \| T_{UICC})$과 AAA와 미리 공유되어 있는 임시ID인 $cTID_{UICC}$를 포함한 $M_1=\{A,\ T_{UICC},\ MAC_{UICC},\ cTID_{UICC}\}$를 MS와 BS를 거쳐 AAA에 보낸다.

(UICC ⇒ MS)

EAP Response/Identity(M_1)

(MS ⇒ BS)

PKM-REQ[EAP-Res./Identity(M_1)]

(BS ⇒ AAA)

DER(EAP Res./Identity(M_1))

Step 3 : AAA는 수신한 $cTID_{UICC}$가 데이터베이스에 있는지 검색한다. 데이터베이스에는 각 가입자 $cTID_{UICC}$와 $pTID_{UICC}$가 저장되어 있다. 이렇게 $pTID_{UICC}$를 유지해 만약 동기화 문제가 발생하면 이전 아이디를 검색해 봄으로써 T_{UICC}의 동기화 문제를 해결할 수 있다. AAA는 MAC_{UICC}을 검증하고 타임스탬프인 T_{UICC}의 유효성을 확인한다. AAA는 새로운 $nTID_{UICC}$와 N_{AAA}를 생성한다. $nTID_{UICC}$는 데이터베이스의 현재 임시 ID필드에 저장되고 $cTID_{UICC}$는 이전 임시 필드에 저장된다. 그리고 AAA는 랜덤값 $b \in Z_P$를 선택하고 B와 $MAC_{AAA} = f_K^1(B \| N_{AAA})$과 $TK = f_K^5(A^b \| N_{AAA})$ 그리고 $AUTH = MAC_{AAA} \| AMF$를 생성하고 BS와 MS를 거쳐 UICC에게 $M_2 = \{TK, AUTH, N_{AAA}, B\}$를 전송한다.

(AAA ⇒ BS)

DEA(*EAP-Req.*(M_2))

(BS ⇒ MS)

PKM-RSP[*EAP-Req.*(M_2)]

(MS ⇒ UICC)

User Auth. Req.[M_2]

Step 4 : AAA로부터 M_2를 받은 UICC는 MAC_{AAA}을 검증하고 TK를 생성한다. 그리고 다음에 사용할 임시 ID를 계산하고 TK와 함께 저장한다. 마지막으로 UICC는 $MAC_{UICC}' = f_{TK}^1(B^a \| N_{AAA})$를 생성해 $M_3 = \{MAC_{UICC}'\}$AAA에게 보낸다.

(UICC ⇒ MS)

EAP-Response[M_3]

(MS ⇒ BS)

PKM-REQ[*EAP-Res.*(M_3)]

(BS ⇒ AAA)

Step 5 : AAA는 M_3를 검증한다. 그리고 CK와 IK를 생성한다. 그 후 실제 통신에 사용될 ID인 $TMSI$를 생성한고 이를 포함한 $M_4 = \{\{TMSI, N_{AAA}\}\}_{TK}$를 UICC에게 전송한다.

(AAA ⇒ BS)

DEA(*EAP-Req*(M_4))

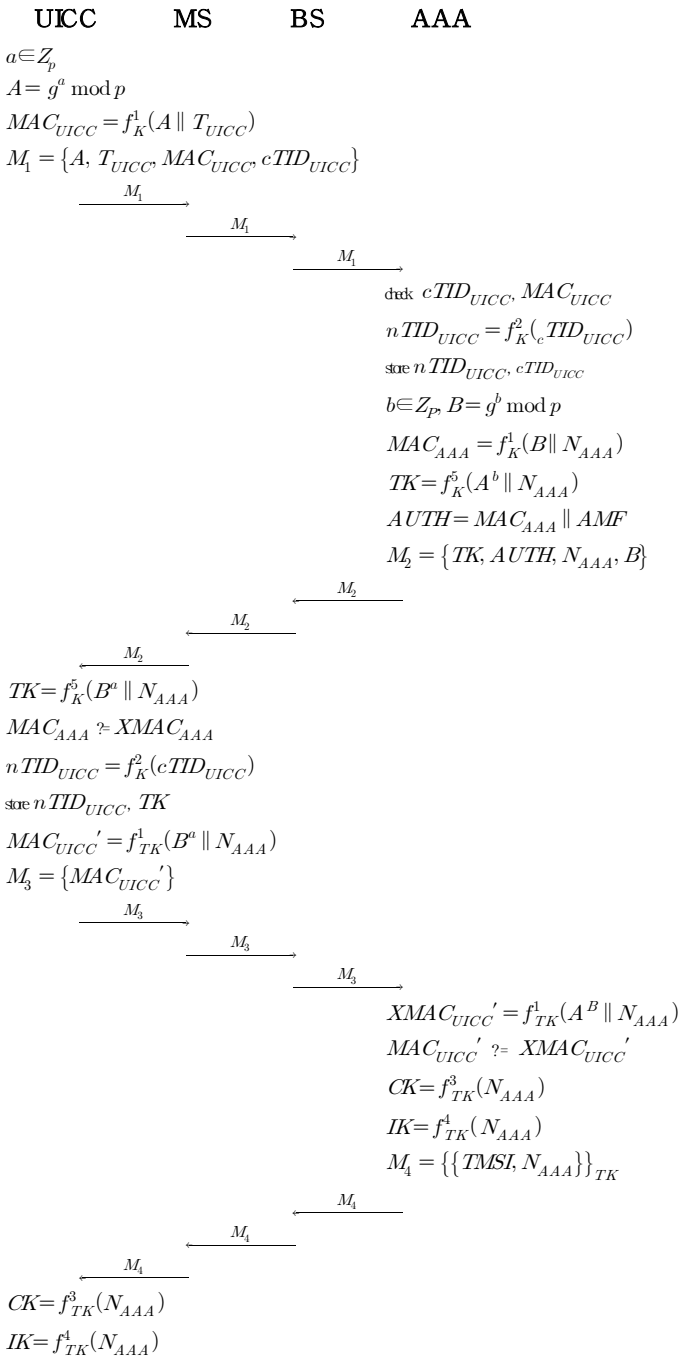
DER(*EAP-Res.*(M_3)

(BS ⇒ MS)

PKM-RSP[*EAP-Req*(M_4)]

(MS ⇒ UICC)

EAP Request/(M_4)



(그림 3) 제안하는 프로토콜

Step 6 : UICC는 M_4를 복호화하고 CK와 IK를 계산한다. 그리고 UICC와 AAA는 이 키들을 이용하여 안전한 통신을 할 수 있다.

4. 안전성 분석

본 장에서는 프라이버시 보호 문제, 인증서버의 저장공간 오베헤드 문제, 전방향 안전성 문제, 재전송공격에 관하여 본 논문에서 제안한 프로토콜의 안전성을 분석한다.

◈ 프라이버시 보호 문제 : 제안하는 프로토콜은 인증서버와 미리 공유하고 있는 비밀키 K를 이용해 새로 생성한 임시 ID인 TDI_{UICC}를 전송하기 때문에 이전 프로토콜과는 달리 프라이버시 보호가 강화된다.

◈ 인증서버의 저장공간 오버헤드 문제 : 다수의 AV를 사용함으로써 인증서버에 저장공간 오버헤드 문제점을 가졌으나 제안방식에서는 AV사용 대신 타임스탬프를 이용해 TK를 생성하여 인증과정에 이용함으로써 문제점을 해결하였다.

◈ 전방향 안전성 문제점 : 비밀키 K가 장시간 노출 되었을 때 비밀키 K를 이용해 3자가 세션키를 얻을 수 있는 문제점을 제안방식에서는 Diffie-Hellman 기법을 사용하여 TK를 생성하고 CK, IK생성시 이용함으로써 해결하였다.

◈ 재전송공격(Replay Attack) : 제안방식에서는 MAC값에 포함된 타임스탬프와 난스를 통해 메시지의 최근성을 검증하기 때문에 공격자의 재전송 공격에 안전하다.

5. 결론

본 논문에서는 기존에 제안된 UICC기반의 EAP-AKA 프로토콜의 문제점을 해결하기 위한 새로운 UICC기반의 EAP-AKA프로토콜을 제안하였다. 먼저 기존 제안된 UICC기반의 EAP-AKA프로토콜의 문제점인 프라이버시 보호 문제와 인증서버 저장공간 오버헤드, 전방향성 제공 문제점에 대해 제시하고 이를 해결하기 위한 새로운 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜은 향후 UICC 기반의 Wibro네트워크에서의 보다 안전한 서비스를 제공하기 위한 기본 프로토콜로 사용될 수 있을 것이다.

참고 문헌

[1] RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement(EAP-AKA)”, January 2006.

[2] 홍대형, 강충구, 조용수, “2.3GHz 휴대인터넷 기술의 국내 표준화”, TTL 저널 Vol.92, No.15, 2004.03

[3] 조석현, 윤철식, “WiBro 시스템에서 보안 기술”, 한국방송공학회지, 1226-7961, Vol.11, No.2, pp.33-41, 2006

[4] 3GPP TS 23. 101 v7.0.0 (2007-06)

[5] 임선희, 이옥연, 전성익, 한진희, “EAP-AKA를 적용한 Wibro무선 네트워크의 인증구조 연구”, 한국통신학회논문지 Vol.31,No.4C, 2006.4

[6] TTAS.KO-06.0110/R1, "휴대인터넷(와이브로TM) 서비스를 위한 상호 인증 절차", 2006.06

[7] 3GPP TS 33.234, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, Wireless Local Area Network(WLAN) interworking security”, June 2005.