UMTS-WLAN-WiBro 연동을 위한 티켓기반의 개선된 EAP-AKA 프로토콜

이경신*, 김대영*, 김상진**, 오희국*

*한양대학교 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학과

An Improved Ticket-based EAP-AKA Protocol for Interworking of UMTS, WLAN, and WiBro

Kyoungshin Lee*, Daeyoung Kim*, Sangjin Kim**, Heekuck Oh*

*Department of Computer Science and Engineering, Hanyang University
**School of Internet Media Engineering, Korea University of Technology and Education

요 약

다양하게 제공되고 있는 무선 네트워크 서비스를 통합하기 위한 보안 연동 기술 개발이 활발히 이루어지고 있다. 통합 보안 연동 기술을 위해 IETF에서 EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement)[8]가 표준으로 제안되었지만 HN(Home Network)이 MS(Mobile Station)를 직접 인증하지 못하고 사용자의 permanent identity가 노출되는 등 여러 보안상의 문제점이 제기되고 있다. 또한 SN(Serving Network)이 필요로 하는 저장 공간이 너무 많고 SN과 HN 사이의 대역폭 낭비, 동기화 문제 등 효율성에 있어서도 문제점이 제기되고 있다. 이 논문에서는 개선한 AKA(*Authentication and Key Agreement*)[12] 프로토콜을 PEAP(Protected EAP)에 적용하여 기존 EAP-AKA보다 안전하고 효율적인 티켓기반의 프로토콜을 제안한다. 제안하는 프로토콜은 HN과 MS 간의 상호 인증을 보장하고 사용자의 permanent identity를 보호하여 안전하고, 계산량과 저장 공간에 있어 기존의 EAP-AKA보다 효율적이다.

I. 서론

무선 네트워크 기술의 발전으로 인해 UMTS(Universal Mobile Telecommunications System)[10]와 WLAN(Wireless LAN)을 중심으로 WiBro(Wireless Broadband Internet)에 이르기까지 다양한 무선 네트워크 서비스가 제공되고 있다. UMTS는 넓은 통신 반경을 가지지만 전송 속도가 떨어지며, WLAN은 빠른 전송속도를 가지지만 통신 반경이 작은 단점을 가진다. WiBro는 전송 속도나 반경 등의 측면에서 UMTS와 WLAN의 중간 영역에 위치한다[11].

최근 이러한 여러 무선 네트워크 서비스의 장단점을 상호 보완하여 통합 무선 네트워크 서비스 체계를 구축하고자 하는 노력이 활발히 이루어지고 있다[13]. 각각의 무선 서비스의 성능 제약을 해결하고 환경에 따라 효율적으로 대역폭을 관리

할 수 있는 통합 무선 네트워크 서비스를 구축함으로써 사용자들은 넓은 통신 반경과 빠른 전송속도를 통해 QoS와 mobility를 제공받을 수 있게 될 것이다. 통합 무선 네트워크 서비스는 인증이나 과금 등의 서비스를 단일화된 방식으로 처리할 수 있어야 하며, 연동 과정에서 끊어짐 없는 통신 서비스를 제공해야 한다[2][14]. 이러한 통합 무선 네트워크 서비스를 안전하게 구축하기 위해 보안 기술이 요구되는데 각 무선 네트워크 서비스

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(ITRC) 지원사업의 결과로 수행되었음.

이 연구에 참여한 연구자는 '2단계 BK21 사업'의 지원을 받았음.

에 대한 보안만이 아니라, 연동되는 네트워크상에서 보안을 제공할 수 있는 새로운 보안 기술이 구축되어야 한다[1][5].

II. 관련 연구

1. AKA 프로토콜

AKA 프로토콜은 UMTS에서의 표준 프로토콜로 MS와 HN, SN으로 구성된다. MS는 자신의 HN과 비밀키 K를 공유하며, 인증벡터와 sequence number를 사용하여 인증과 키 동의를 수행한다. AKA 프로토콜은 크게 두 단계로 나뉘는데, 첫 번째 단계에서는 MS가 자신의 HN에 MS를 등록하고 HN이 SN에게 인증벡터를 나눠준다. 두 번째 단계에서는 SN과 MS 사이의 인증과 키 동의 과정을 수행한다. 그러나 HN이 MS를 직접 인증하지 못하고, HN과 SN사이의 대역폭 오버헤드 문제, SN의 저장 공간 오버헤드 문제 등 안전성과 효율성에 여러 문제점이 제기되고 있다.

2. EAP 프로토콜

EAP 프로토콜은 WLAN에서 기본적으로 사용되는 인증 프로토콜이다. EAP 프로토콜은 인증을 하나의 통일된 인증 프로토콜로 모두 수용 가능하도록 표준화한 프로토콜로써, 헤더에 다양한 종류의 인증방식을 명시할 수 있도록 하여 확장성을 부여한다.

3. PEAP 프로토콜

PEAP(Protected EAP)는 EAP 인증 방식 중의 하나로 TLS 터널 상에서 사용자를 인증하는 프로토콜이다[14]. PEAP는 완전한 PKI 구조가 되어 있지 않은 무선 LAN 환경에서 서버 인증서만을 사용하여 단말들은 인증서가 없이도 상호인증이 가능하다. 단말은 먼저 MS와 인증 서버간의 TLS 보안 채널을 설정하고, MS는 PEAP 인증서버의 인증서로 서버를 인증한 후, 안전한 TLS 채널 상에서 EAP 기반의 인증방식을 사용하여 사용자 인증절차를 수행한다.

4. EAP-AKA 프로토콜

일반적으로 WLAN과 WiBro의 인증에는 PPP (Point-to-Point) 인증 방식에 기반한 EAP가 사용되고 있으며, UMTS의 인증에는 AKA방식이 사용되고 있다. IETF의 표준인 EAP-AKA 인증은 UMTS, WLAN를 사용하는 사용자가 표준 인증인 AKA 방식을 이용하여 동일하게 인증될 수 있는 모델을 보여준다.

EAP-AKA 인증은 기존 AKA 인증에 EAP 개념을 도입하여 사용자의 단일 인증을 통한 편의성, 호환성 및 보안이 강화되었으나, 기존 EAP가 가지는 문제점과 AKA가 가지는 문제점들을 그대로 가지고 있다.

III. 제안하는 프로토콜

본 논문에서는 EAP-AKA에서의 보안 취약점을 개선하여 통합 무선 네트워크 서비스 시스템에서 안전하고 효율적인 티켓기반의 개선된 EAP-AKA를 제안하고자 한다. 제안하는 프로토콜은 크게 두 단계로 나뉘는데, 첫 번째 단계에서는 PEAP 프로토콜을 그대로 적용하여 기존의 EAP-AKA보다 안전한 채널 상에서의 통신을 제공한다. 두 번째 단계에서는 첫 번째 단계에서 PEAP 프로토콜을 통해 제공되는 안전한 채널 상에서 기존의 AKA 프로토콜을 개선하여 티켓기반의 안전하고 효율적인 프로토콜을 제안한다. 제안하는 프로토콜은 기존의 EAP-AKA 프로토콜이 사용하던 인증벡터 대신 티켓키 방식을 사용하며, sequence number를 사용하지 않는다.

UMTS와 WLAN, 그리고 WiBro 간의 통합 연동 모델에서 MS와 HLR은 서로 비밀키 K를 공유하고 있으며, 인증서버와 HLR은 안전한 채널이 형성되어 있다고 가정한다. 제안하는 프로토콜의 인증절차는 <그림 1>과 같다.

- 단계1. AP가 MS에게 EAP Request/Identity 메시지를 전송
- 단계2. MS가 AP에게 익명의 identity인 anonymous를 전송
- 단계3. AP는 MS의 EAP Response/Identity를 인증서버에 전송
- 단계4. 인증서버가 MS에게 인증서버의 인증서를 전송
- 단계5. MS는 서버의 인증서를 통해 인증서버를 인증
- 단계6. MS가 Premaster secret를 생성하여 인증서버에게 전송
- 단계7. Premaster secret으로 MS와 인증서버가 각자 TLS master secret을 생성
- 단계8. TLS master secret으로 MS와 인증서버가 각자 key material TLS용 암호를 생성
- 단계9. 생성한 key material TLS용 암호를 통해 안전한 TLS 세션 구축

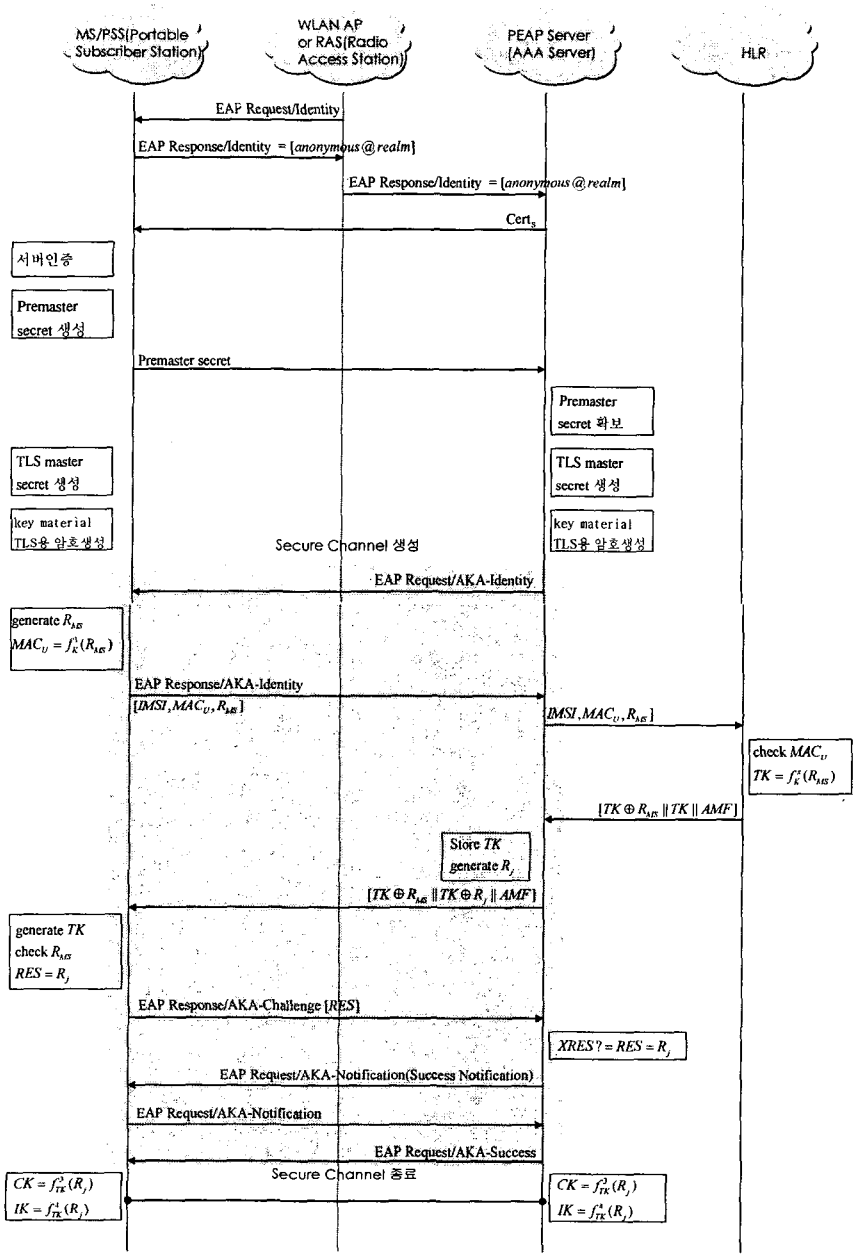

그림 1: 제안하는 프로토콜

- 단계10. 인증서버가 MS에게 EAP Request/AKA-Identity를 통해 identity 요청
- 단계11. MS가 인증서버에게 안전한 세션상에서 자신의 IMSI와 MS가 생성한 random number R_{MS}, MAC값 전송
- 단계12. 인증서버가 MS에게서 전달받은 MS의 IMSI와 , MAC값을 HLR에게 전송
- 단계13. HLR이 MAC값을 통해 무결성을 확인하고 전달받은 R_{MS}로 티켓키 TK를 생성하여 TK와 R_{MS}, AMF를 인증서버에 전송

- 단계14. 인증서버는 TK를 저장하고 TK와 R_{MS}를 XOR한 값과 TK와 R_j를 XOR한 값, AMF를 MS에게 전송
- 단계15. MS는 R_{MS}로 티켓키 TK를 생성하고, 인증서버로부터 받은 값을 통해 TK와 R_{MS}가 맞는지 확인하고 XRES로 R_j를 계산
- 단계16. MS는 계산한 R_j를 EAP Response /AKA-Challenge를 통해 인증서버에 전송
- 단계17. 인증서버는 자신이 계산한 XRES와 MS가 생성한 RES가 일치하면 EAP Request /AKA-Notification(Success Notification)을 MS에게 전송
- 단계18. MS는 응답으로 EAP Response/ AKA-Notification을 전송
- 단계19. 인증서버는 MS에게 EAP Request/ AKA-Success를 통해 인증이 성공적으로 이루어졌음을 알림
- 단계20. 서버와 MS는 R_j를 통해 통신에 사용할 CK와 IK를 각자 계산

IV. 안전성 및 효율성 분석

제안하는 프로토콜은 크게 TLS 채널 설정단계와 사용자 인증단계로 구성된다. 첫 번째 단계인 TLS 채널 설정 단계에서는 MS와 인증서버 간의 TLS 보안 채널을 설정하면서 MS는 PEAP 인증서버의 인증서로 서버를 인증한다. 하지만, 서버 인증서만 사용하였기 때문에 아직 서버 입장에서는 MS를 인증한 것이 아니다. 기존의 EAP-AKA 프로토콜에서는 MS가 서버에게 인증받기 위해 MS의 permanent identity를 노출시키는 문제점을 해결하기 위해 PEAP 프로토콜을 적용하여 permanent identity 대신 anonymous라는 익명의 identity를 전송한다. 그리고 안전한 TLS 채널이 생성된 뒤에 두 번째 단계인 사용자 인증 단계에서 MS의 permanent identity를 전송하는 사용자 인증절차를 수행하여 사용자의 개인정보를 보호하였다. 그리고 AKA 프로토콜을 개선하여 HN이 R_{MS}와 MS의 MAC을 검증함으로써 MS를 인증할 수 있도록 하여 HN과 MS 간의 상호 인증을 보장하며, 기존의 EAP-AKA 방식이 사용하던 인증벡터 대신에 티켓키 방식을 사용하여 SN이 필요로 하는 저장 공간을 줄이고 SN과 HN 사이의 대역폭 낭비를 줄이며, 프로토콜의 연산이 대부분 XOR로 이루어지기 때문에 계산량에 있어서도 기존의 방식보다 효율적이다. 또한 sequence number를 사용하지 않기 때문에 동기화문제를 해결하였다.

V. 결론

통합 무선 네트워크 서비스를 안전하게 구축하기 위해 보안 기술이 요구되는데 각 무선 네트워크 서비스에 대한 보안만이 아니라, 연동되는 네트워크상에서 보안을 제공할 수 있는 새로운 보안 기술이 구축되어야 한다.

본 논문에서는 IETF의 UMTS와 WLAN간의 보안 연동 프로토콜의 표준인 EAP-AKA를 PEAP 프로토콜을 적용하여 안전한 채널을 생성한 후, 바로 인증서버가 MS를 인증하도록 하여, 사용자의 permanent identity는 노출되지 않도록 보호하면서, 인증되지 않은 MS와의 불필요한 연산은 줄이도록 하였따. 또한 PEAP 프로토콜로 안전한 채널을 보장한 상태에서 AKA 프로토콜을 개선하였다. 제안하는 프로토콜은 인증벡터 대신 티켓키 방식을 사용하여 SN이 필요로 하는 저장 공간을 줄이고 SN과 HN 사이의 대역폭 낭비를 줄이며 동기화 문제를 해결하여 기존의 EAP-AKA 방식보다 간단하고 안전하며 효율적인 프로토콜을 설계하였다.

참고문헌

[1] 3GPP TS 33.234 "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3G Security; Wireless Local Area Network(WLAN) interworking Security; (Release 7)," 2006.

[2] Y. C. Ouyang and C. H. Chu, "A Secure Context Transfer Scheme for Integration of UMTS and 802.11 WLANs," in *IEEE International Conference on Networking, Sensing and Control.* Vol 1, pp. 559-564, 2004.

[3] C. M. Huang and J. W. Li, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption," in IEEE International Conference on Advanced Information Networking and Applications, Vol 19

[4] 3GPP TR 23.934 "3rd Generation Partnership Project; Technical Specification Group

Services and System Aspects; 3GPP System to Wireless Local Area Network(WLAN) Interworking; Functional and Architectural Definition(Release 6)," 2002.

[5] 3GPP TS 23.234 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network(WLAN) Interworking; System Description(Release 6)," 2004.

[7] RFC 3748 "Extensible Authentication Protocol(EAP)," 2004.

[8] draft-arkko-pppext-eap-aka-12.txt "Extensible Authentication Protocol for UMTS Authenticationand Key Agreement(EAP-AKA)," 2004.

[9] 3GPP TS 35.205~208 "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*;(Release 5)," 2002.

[10] http://www.3gpp.org/

[11] http://www.etsi.org/

[12] http://www.ietf.org/

[13] 김영세, 이정우, 한진희, 신진아, 전성익, "무선 네트워크 연동 보안 기술 동향", 전자통신동향분석, Vol 20, 2005.

[14] draft-kamath-ppext-eap-mschapv2-01.txt>, "Microsoft EAP CHAP Extensions", 2004