공중 무선랜의 이동성 향상을 위한 인증 모델 연구

김관연*, 한국민*, 김신효**, 정병호**, 박세현*

*중앙대학교 전자전기공학부 인터넷세계 보안 연구실

**한국전자통신연구원

A Study of Authentication Model for Mobility elevation of Public Wireless LAN

Gwan Yeon Kim*, Kuk Min Han*, Shin Hyo Kim**, Byung Ho Jung**, Se Hyun Park*

*School of Electrical and Electronic Engineering, Chung-Ang University, Cipher Internet-World Lab.

**Electronics and Telecommunications Research Institute

요 약

공중무선랜은 오늘날 빠르게 증가하고 있는 무선인터넷 서비스에서 빠른 전송속도와 저렴한 설치비용 등으로 빠르게 성장하고 있는 중요한 기반요소로 평가되고 있다. 하지만 무선랜 시장에 대한 기대 뒤에는 보안에 대한 우려 또한 높아지고 있으며 로밍이나 핸드오버에 대한 수요가 커지고 있으나 실제로는 서비스 반경이 작고, 간섭에 의해 서비스 품질을 보장하기 어려우며 사용자 인증, 접근제어, 과금 부분에 있어 믿을 만한 초기 단말 인증이 보장되지 않아 도메인간 연동 문제가 쉽지 않다.

이러한 문제를 보완하여 초고속 멀티미디어 서비스를 제공할 수 있는 Mobile IP 기반 로밍 및 핸드오버에 대한 기반 기술 및 Mobile IP에 적용되는 사용자 인증 서비스에 대한 기반기술인 802.1x를 비롯하여 802.11f, Mobile IP등을 고려하여 이동성이 보장된 공중 무선랜 서비스를 위한 인증 방안을 제안하고 검증하며 제안된 방안은 차후로 ALL-IP 기반의 차세대 3G 이동통신망에서 이용될 수 있는 AAA 방안으로 확장하여 적용이 가능한 AAA 모델의 기반기술이 될 것이다.

I. 서론

공중무선랜은 오늘날 빠르게 증가하고 있는 무선인터넷 서비스에서 빠른 전송속도와 저렴한 설치비용 등으로 빠르게 성장하고 있는 중요한 기반요소로 평가되고 있다. KT를 비롯한 많은 ISP 업체들이 차세대 이동통신의 한 수단 또는 대체로서 공중 무선랜 서비스를 생각하고 있으며 현재 실제 공중망 서비스를 하고 있으나 아직은 사용자의 편의성을 위해 인증이나 접근제어 부분에 있어 상당부분 보안적 취약점을 가지고 있다. 그러나 무선랜은 이러한 어려움에 비해 저렴한 설치비용, 이동성 및 설치의 용의성과 같은 효율적인 이득으로 인해 빠른 속도로 성장하고 있다.

이러한 시대적 흐름에 맞추어 Seamless한 ALL-IP[1][2] 초고속 멀티미디어 서비스를 제공할 수 있는 Mobile IP 기반 로밍 및 핸드오버에 대한 기반 기술 및 Mobile IP에 적용되는 사용자 인증 및 과금 기능 등의 각종 인증서비스에 대한 기반기술을 이용하여 이동성이 보장된 공중 무선랜 서비스를 위한 인증 방안을 제안하고 검증하는 것이 본 연구의 목적이며 본 연구 결과를 바탕으로 차후에는 ALL-IP 기반의 차세대 3G 이동통신망에서 이용될 수 있는 AAA 방안으로 확장하여 적용이 가능한 AAA 모델을 제안한다.

본 연구에서 표준의 내용을 벗어나지 않는 범위 내에서 기존의 유선 네트워크와도 잘 연동되며 전반적인 보안적 요소는 유선 네트워크에 준하도록 구성되도록 하였다.

* 본 논문은 한국과학재단 목적기초(R01-2001-00303) 및 한국전자통신연구원의 지원으로 수행되었음.

II. 무선랜 구조 및 취약점 분석

초기 무선랜은 1~2Mbps를 지원하는 수준이었다가 최근에는 11Mbps와 54Mbps를 지원하는 무선랜이 각각 IEEE 802.11b, IEEE 802.11a로 표준화되어 점차 요구되어 가고 있는 대용량 트래픽

의 고속 전송에 부합되고 있는 모습을 갖추고 있다.

하지만 무선랜 시장에 대한 기대 뒤에는 보안 문제가 지적되고 있다. 실제 유선 네트워크와는 달리, 무선 네트워크는 공중으로 데이터를 전송하기 때문에 일반적으로 조직체의 물리적인 경계선 너머로 뻗어나갈 수 있으며 특히, 강력한 지향성 안테나를 사용하는 경우, 무선랜은 설계된 건물들을 벗어난 먼 곳까지 도달할 수 있다. 이러한 경우 기존의 물리적인 보안 제어 기능이 무력화되는 환경이 만들어진다.

그리고 무선랜의 오픈구조에서는 무선 주파수 범위 내의 모든 사람이 패킷을 볼 수 있기 때문에 누구든지 이 문제점을 이용하여 임의의 무선랜 상에서 돌아다니는 모든 패킷을 받아서 저장할 수 있다. 그리고 연결되어 있는 통신에 끼여드는 것도 쉬우며 간단한 재밍 트랜스미터만 있으면 통신을 불가능하게 만들 수 있다. 예를 들어, AP로 액세스를 계속 요청하면 그 요청이 성공하든 하지 않든 간에 결국 그 AP의 가용 무선 주파수대가 고갈되어 네트워크가 다운되어 버린다. 이러한 의도적이거나 무의도적인 DoS(denial-of-service) 공격으로 인해 무선랜 장치를 사용할 수 없게 될 수 있다.

이러한 취약점을 개선하고자 무선랜 표준인 IEEE 802.11[3]에서 보안을 위한 옵션으로 'WEP[3]'이라는 것을 제안하고 있다. WEP는 'Wired Equivalent Privacy' 약자로 유선랜에 상당하는 프라이버시를 제공하기 위해 공유키 인증과 암호화 알고리즘을 규정하고 있다.

WEP을 이용하는 공유키 인증방식은 IEEE 802.11과는 독립적인 안전한 채널을 통해 사전에 단말에 전달된 공유키를 이용하여 동일한 키를 가지고 있는 단말을 인증하는 방법이다. 그러나 이러한 WEP에서는 RC4 알고리즘과 키를 사용하는 것에 대해 설명하지만, 구체적인 키 배포 방식은 규정하지 않는다. 또한 IV의 취약점을 공격하는 FMS공격[4]에 의해 문제가 생기게 된다.

이러한 문제점은 다음절에서 서술하는 사용자 기반 인증을 제안하고 있는 802.1x를 이용하면 획기적으로 개선이 가능하다.

III. 802.1x기반의 인증 및 접근제어

IEEE에서 제안된 Port-Based Network Access Control (IEEE Std 802.1X-2001[5])은 포트를 기준으로 한 IEEE 802 랜 기기들로 구성된 통신망 접근 제어의 조항에 대한 일반적인 방법을 지정하며 서로 연결된 IEEE 802 랜 기기들을 위한 호환된 인증과 허가 메커니즘을 제공한다. 이를 무선랜에 적용하여 사용한다면 다음과 같은 단계를 거쳐 인증 및 접근제어를 수행할 수 있다.

아래 그림 1에서처럼 우선 사용자가 포트를 사용하기 위해 802.1x 기능을 수행하는 AP로 단말에서 승인을 요청하면, AP는 단말의 인증 데이터를 RADIUS[6] 서버로 보낸다. RADIUS 서버는 승인 결과의 암호키를 AP로 보내고 이것은 단말로 다시 전송되면서 단말은 해당 포트를 접근할 수 있는 권한을 얻고 AP는 이를 허용하여 인증받은 사용자만 서비스를 이용하게 한다.

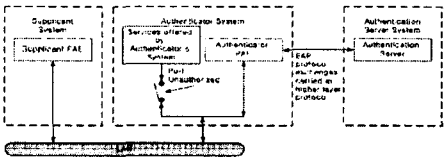

그림 1: Model of Port-Based Network Access Control Entities

802.1x의 장점을 들자면 EAP (Extensible Authentication Protocol) [7] 구조를 도입하여 RADIUS와 쉽게 결합할 수 있으며, 어떤 링크 계층에서도 동작할 수 있게 준비돼 있다는 것이다. 따라서 802.1x 기반의 네트워크에서는 기업의 보안 정책을 그대로 네트워크 하드웨어에 적용시키는 응용 기술을 사용할 수 있다. 또한 네트워크를 사용하기 위해 사용자별로 인증을 받아 접속해야 하므로, 현재 문제가 되고 있는 DoS(Denial of Service) 공격을 막는데도 도움을 줄 수도 있다.

이상의 802.1x에 대해 서술하였는데 본 연구의 목표인 이동성이 보장된 공중 무선랜에서의 AAA 모델을 제안하기 위해서는 802.1x에서 부족한 단말의 잦은 이동에 따른 이동성을 보장해줄 방안이 필요하다.

IV. 이동성 보장을 위한 보안사항

이동통신망을 이용한 무선 인터넷 가입자가 2000만명을 훌쩍 넘어서고, 공중 무선랜 서비스의 등장 등으로 무선 인터넷 이용이 확대됨에 따라 무선 인터넷은 폭발적인 성장이 기대되고 있다. 이러한 무선 인터넷 서비스에서는 이동 중에서 끊어지지 않고 통신할 수 있는 Seamless 핸드오프가 보장되어야 있다. 특히 IMT-2000망과 같은 3G이상의 이동통신망은 ALL-IP 환경을 지원하기 때문에 IP망에서의 이동성 지원 기술인 Mobile IP가 휴대전화, PDA, 노트북 등 모든 단말기에 필수적으로 적용될 것으로 예측된다.

그러나 Mobile IP를 무선랜에 적용하기에는 어려움이 있다. 그중 가장 큰 이유는 AP의 특성상 서비스 반경이 100m에서 최대 300m내외로 이동통신 네트워크에 비해 커버리지가 작고, 간섭에 의해 서비스 품질을 보장하기 어려우며 빠른 속도로 이동하는 무선랜 단말에 대한 실시간 서비

스 제공에는 어려움이 있다. 즉 핸드오프 시 발생할 수 있는 패킷 손실이나 지연에 의해 VoIP나 멀티미디어 서비스와 같은 실시간 서비스에서는 성능저하가 나타난다는 것이다.

따라서 이를 위해 로우 레이턴시 핸드오프(low latency handoff)[8], 패스트 핸드오프 (Fast MIPv6)[9] 등의 새로운 프로토콜과 함께 Mobile IP 등록 영역을 지역화해 등록과정에서 사용되는 신호를 줄여 불필요한 오버헤드와 시간을 단축시킴으로써 Seamless 핸드오프를 가능케 하는 마이크로 모빌리티(Micro Mobility) 기술 등이 활발하게 개발되고 있다. 그러나 아직 무선랜에 적용하기에는 어려우며 IEEE 802.11f WG에서 현재 Draft상태에 있는 802.11f[10]를 이용하여 보안하고자 한다.

여기서 사용되는 IAPP[10]는 AP(Access Point) 간의 실시간 정보를 통해 움직이는 단말 장치의 위치가 어디인지 관리해 주어 분산 환경에서 스테이션의 이동에 따른 무선접속장비 간의 로밍을 할 수 있게 해준다.

이 프로토콜의 주요 목적은 이동무선단말에 직접 연관이 있는 데이터의 흐름을 놓치지 않기 위해, 브리지테이블의 빠른 갱신을 보장하며 같은 네트워크 내에 있는 다른 AP(Access Point)에 대한 정보를 넘겨주어 이동무선단말의 빠른 재인증을 허용하기 위한 인증 데이터를 서로 공유하는 데 있다.

V. 이동성이 향상된 AAA 제안

Mobile IP는 Macro Mobility를 지원하기에 적당하고 반면 IAPP는 Micro Mobility를 지원하기 적합한 특성을 가지고 있다. 즉 Mobile IP가 적용된 DC(Domain Controller)와 그 이하 AP들 사이의 IAPP로 구성된 네트워크라면 Macro Mobility 및 Micro Mobility 모두를 적용할 수 있다. 여기서 핵심적인 아이디어는 IAPP의 프레임 워크를 이용하는 단말과 AP에서 동일 도메인 즉 Micro Mobility인 경우에는 기존 IAPP로 적용이 되고 만일 도메인이 달라지는 Macro Mobility인 경우 즉 IAPP에서 이전 AP를 검색하였는데 찾을 수가 없을 때 Mobile IP가 적용되어 Seamless 핸드오프를 적용할 수 있도록 하는데 있다.

그림 2에서 보면 두 가지 시나리오로 설명할 수 있다. 시나리오 A를 보면 하나의 도메인 내에서는 단말이 ①의 과정을 통해 AP로 접속 요청을 하면 AP는 AAA 서버 안에 있는 IAPP 리스트 관리 서버에서 이전 AP의 주소를 알아낼 수 있고 이전 AP에게 IAPP.Move-Request패킷을 보내고 IAPP.Move-Response를 받아 이동에 필요한 정보를 받아낼 수 있다. 그러나 만약 시나리오 B에서처럼 단말이 도메인을 이동한 다음 ②의 과정으로 AP에 접속하게되면 AP는 IAPP 리스트 관리서버에서 이전 AP의 주소를 알아낼 수 없고 그렇게 되면 AP는 이 단말이 다른 도메인에서 왔음을 알고 Mobile IP로 동작한다. 그래서 ③의 과정으로 Seamless 핸드오프를 수행한다.

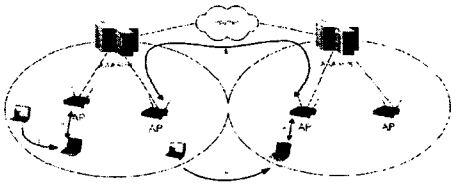

그림 2: Mobile IP와 IAPP의 연동 시나리오

그러나 실제로 IAPP은 2계층에서 링크계층의 이동성만을 보장하기 때문에 서브넷이 다른 곳으로 핸드오프 시 사용할 수 없는 문제가 있어 보완되지 않는 경우 Mobile IP와 연동하기 이렵다.

Seamless한 핸드오프를 위해 IAPP를 다른 서브넷에서도 쓸 수 있도록 확장하여 사용할 수 있도록 제안하였다.

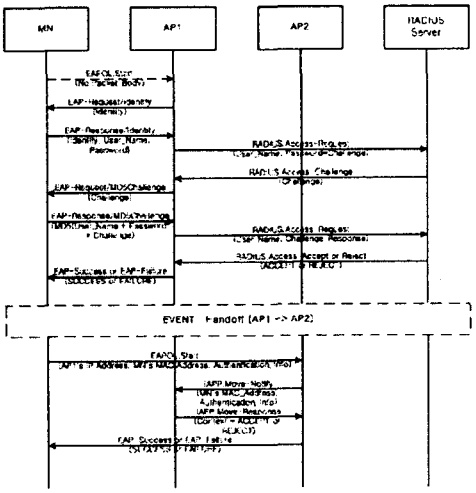

그림 3: 제안된 확장 IAPP 프로토콜

그림 3은 제안된 프로토콜을 이용하여 핸드오프를 수행하는 프로토콜이다. 단말이 AP1에서 사용하다가 AP2로 이동하게 되면 MAC에서의 Reassociation을 수행한 다음 Authentication을 요청하게 되는데 이때 이전 AP1의 IP주소 및 자신이 AP1으로부터 받았던 인증권한의 증거인 인증토큰을 첨부하여 전송한다. 받은 AP2는 이 정보를 이용해 AP1에게 확인하고 단말을 다음번 재인증 기간까지 권한을 주게된다. 그로 인해 빠른 AP간 이동이 가능해지며 인증서버의 부하도 감소하게 된다.

제안된 프로토콜을 이용한 모델은 이전 AP와의 인증 정보 및 연결정보를 이용하여 Seamless 서비스를 제공할 수 있으며 IP기반의 프로토콜로 확장되었기 때문에 추가적인 Mobile IP Agent와

의 연동 프로토콜을 제안함으로써 도메인간 로밍도 가능하다. 또한 단말의 보안적인 인증이 보장되어 과금 시스템과의 연동을 통해 Seamless 서비스를 제공할 수 있을 것이다.

VI. 결론

본 연구에서는 802.1x와 IAPP를 이용한 이동성이 보장된 인증 및 과금 모델을 EAP-MD5 에뮬레이션 프로그램과 IAPP 에뮬레이션 프로그램, 그리고 RADIUS 서버 프로그램의 연동을 이용한 시뮬레이션을 통해 검증하였다.

기존의 모델과 본 연구에서 제안된 모델을 시나리오로 제시하고, 그에 따른 시뮬레이션을 통해 기존의 모델과 제안된 모델의 성능을 평가하였다. 이러한 성능 평가를 통해서 본 연구에서 제안한 모델의 효율성을 확인하였고, IAPP 프로토콜에 인증 기능을 추가하여 AP간의 인증 정보 교환을 통해 RADIUS 서버로부터의 재인증 절차에서 오는 오버헤드를 줄일 수 있었고, 또한 핸드오프가 일어나기 전에 MN가 속해 있던 이전의 AP 정보를 새로 association 하는 AP에게 전달해 줌으로써, 새로운 AP가 이전의 AP 정보를 얻어오는 과정에서 발생하는 오버헤드를 효과적으로 줄일 수 있음을 확인하였다.

따라서, 본 연구에서 제시한 모델을 통해 AP간 인증 정보 및 과금 정보를 IAPP 프로토콜을 이용하여 전달함으로써 빠른 핸드오프를 지원하고 이동환경에서 실시간 과금을 실현할 수 있는 기반 기술이 될 수 있을 것으로 기대된다.

참고문헌

[1] v3.0 Wireless IP Network Standard (3GPP2 TSG-P P.S0001-A)

[2] Wireless IP Architecture Based on IETF protocols
(3GPP2 TSG-P P.R0001)

[3] ISO/IEC 8802-11 Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

[4] http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

[5] Port-Based network Access Control (IEEE 802.1x-2001)

[6] Remote Authentication Dial In User Service (RFC2865)

[7] PPP Extensible Authentication Protocol (RFC2284)

[8 Low Latency Handoffs in Mobile IPv4 (dratf-ietf.mobileip-lowlatency-handoffs-v4-04.txt)

[9] Fast Handovers for Mobile IPv6 (draft-ietf-mobileip-fast-mipv4-04.txt)

[10] IEEE Std.802.11f/D3.1, Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol across Distribution Systems Supporting IEEE 802.11 Operation