공중 무선랜 망에서 이동성을 고려한 통합 인증 모델 연구

김진택*, 김관연*, 박세현*

*중앙대학교 전자전기공학부

A Study of Integrated Authentication Model considering Mobility in Public Wireless LAN Network

Jin-taek Kim*, Gwan-yeon Kim*, Se-hyun Park*

*Department of Electrical and Electronics Engineering, Chung-Ang Univ.

요 약

무선랜은 현재 무선 네트워크에서 매우 중요한 역할을 차지하며, 앞으로의 차세대 무선 통합네트워크에서 또한 그 비중이 매우 높아 질 것이다. 특히 핫스팟과 같은 공중망 서비스의 확산으로 무선 인터넷 등의 차세대 정보 컨텐츠 산업의 중요한 매체로 부각되고 있다. 이에 부합하여 무선랜 서비스에 있어 사용자의 프라이버시(Privacy) 및 접근제어(Access Control), 인증(Authentication), 과금(Accounting), 빌링(Billing) 등의 다양한 보안 문제가 중요한 이슈로 대두되고 있다. 본 논문에는 공중 무선랜에서의 이동성이 고려된 인증 모델을 여러 국제 표준에 맞추어 제안하고, 그에 대한 검증 결과를 함께 제시한다. 제안된 모델은 상호 연동성 및 호환성을 보장하기 위해 Diameter를 기반 기술로 사용하였다.

I. 서론

제 3세대 이동 통신망인 IMT-2000의 서비스는 고가의 전용 단말기 및 서비스 이용료와 늦어진 상용서비스 시기로 인해 시장 진입에 어려움을 겪고 있다. IMT-2000 서비스 사업자들은 원활한 시장 진입과 수익성 창출을 위해 기존 공중 무선랜(Wireless LAN) 사업자와의 협력하여 넓은 커버리지와 높은 속도, 저렴한 가격을 만족시키고자 무선랜과의 연동을 시도하고 있다. 있다. 이러한 노력에 발맞추어 현재는 고속 데이터 전송이 가능한 무선랜의 장점과 이동성 및 넓은 서비스 범위가 보장되는 이동통신의 장점만을 결합하여 2.3 GHz 대역의 휴대 인터넷(Wireless MAN)에 대한 논의 또한 활발히 이루어지고 있다. 이러한 배경은 무선랜은 꾸준히 성장할 수 있는 토대를 마련하며, 관련 업계가 꾸준히 기술 개발과 통합 솔루션, 보안등에 관심을 기울이게 하는 원동력을 제공하고 있다. 또한, 공중 무선랜 서비스는 기존 이동전화를 이용한 방법에 비해 값싼 초고속 인터넷 서비스를 이용할 수 있기 때문에 수요가 지속적으로 증가하여 상당한 시장을 형성하고 있다. 그러나 무선랜은 IP 네트워크이기 때문에 인증·접근제어·과금이 복잡하고 표준화 되지 않아 차세대 이동통신과의 연동에 대한 어려움이 있다. 따라서 인증·접근제어·과금에 대한 해결책 제시가 시급히 요구되고 있다.

본 논문에서는 seamless한 ALL-IP[1][2] 기반의 초고속 멀티미디어 서비스를 제공이 가능한 Mobile IP[3][4]를 이용한 로밍 및 핸드오프에 대한 기반 기술 및 Mobile IP에 적용되는 사용자 인증 및 접근제어 등 각종 인증서비스에 대한 기술을 이용하여 이동성이 보장된 공중 무선랜 서비스를 위한 인증 및 접근제어 방안을 제안하고 검증하는 것이 본 연구의 목적이다. 제안된 AAA 방안의 대상이 되는 무선랜 구조 및 프로토콜은 802.11a[5]을 따라 원칙적으로 IP 계층 이하는 변경하지 않는다. 따라서 MAC 계층에서 발생하는 초기 인증과정과 같은 부분으로 인한 부분은 연구 범위 밖이다. 표준의 내용을 벗어나지 않는 범위 내에서 변경이 이루어지며 기존의 유선 네트워크와의 상호 연동성에 대해서도 고려된다. 본 연구

결과는 차후에 ALL-IP 기반의 차세대 무선 통합 네트워크에서 이용될 수 있는 AAA 방안으로 확장하여 적용 될 수 있다.

II. 인증과 접근제어

1. 기존 무선랜의 인증 및 보안 문제

유선 네트워크와는 달리, 무선 네트워크는 공중으로 데이터를 전송하며 일반적으로 조직체의 물리적인 경계선 너머로 뻗어나갈 수 있다. 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. 또한 현재의 무선랜의 구조에서는 무선 주파수 범위 내의 모든 사람이 패킷을 볼 수 있는 오픈 네트워크이기 때문에 예를들어, 랩탑 컴퓨터와 TCPDUMP 혹은 패킷 스니퍼와 같은 프로그램만 있으면, 누구든지 이 문제점을 이용하여 임의의 무선랜 상에서 돌아다니는 모든 패킷을 받아서 저장할 수 있다.[6, 7, 8, 9] 그리고 연결되어 있는 통신에 끼여드는 것도 쉬우며 간단한 재밍 트랜스미터(jammer)만 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.

2. 무선랜 인증 및 보안 해결책

무선랜의 보안은 크게 두 가지 측면에서 접근할 수 있는데, 승인된 사용자에게만 네트워크 접속을 허용하는 보안 방식과 스니퍼 등의 네트워크 분석기를 통해 무선랜 데이터 내용 자체를 몰래 보는 행위를 방어해주는 보안 방법이 있다.

이 중 기존 무선랜에 접속하는 방법 중에서 가장 안전한 방법은 이더넷 어드레스인 MAC(Media Access Control) 어드레스의 리스트를 이용해 정식 사용자의 데이터만을 통과시키는 방법이다. 하지만 MAC 어드레스는 손쉽게 관찰이 가능하고 쉽게 조작이 가능하기 때문에 쉽게 정식 사용자의 MAC 어드레스가 유출될 수 있다. 하지만 요즘과 같이 무선랜이 대형화되는 과정에서 MAC을 이용한 물리적 카드의 보안이 확실하다 하더라도 정상적인 MAC 어드레스의 리스트를 서비스하는 네트워크 분배에 문제가 더 심각해질 수 있다. 모든 업체의 AP는 MAC 어드레스를 보유하는데 한계가 있으며, 이러한 AP의 MAC 어드레스 지원 한계가 이동성을 위한 영역의 확장성 한계로 작용된다. 특히 무선랜 서비스를 하는 업체에게는 이런 확장성의 한계는 치명적일 수 있다. 따라서 이런 한계를 해결하는 방법으로 AP 간에 MAC 어드레스를 공유하는 대책이 논의되기도 한다.

다른 방법인 허가된 사용자만 네트워크를 접속하는 방법에는 여러 가지가 있지만 그중 하나는 SSID(Service Set ID)로 알려진 네트워크 이름을 사용하는 것이다. 이는 특정 사용자 그룹이 특정 AP들을 사용하는데 주로 이용되는데, AP와 사용자의 랜카드에 동일한 네트워크 이름을 등록하면 서비스를 받을 수 있다. 이는 네트워크에 접속하기 위한 공동의 패스워드로 이해해도 좋다. 물론 여러 사람이 공유하는 패스워드는 보안에 대한 신뢰도가 낮다는 단점이 있다.

현재 이러한 무선랜 보안에 대한 우려 속에서 여러 가지 해결책들이 나오고 있으며, 이 중 IEEE 802.1x를 해결책으로 제시하는 업체들이 늘어나고 있다. IEEE에서 제안된 Port-Based Network Access Control (IEEE Std 802.1X-2001[10])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. 간단하게 서술한다면 사용자가 포트를 사용하기 위해 802.1x 기능을 수행하는 AP로 단말에서 승인을 요청하면, AP는 단말의 인증 데이터를 RADIUS 서버로 보낸다. RADIUS 서버는 승인 결과의 암호키를 AP로 보내고 이것은 단말로 다시 전송되면서 단말은 해당 포트를 접근할 수 있는 권한을 얻고 AP는 이를 허용한다. 802.1x의 장점을 들자면 EAP(Extensible Authentication Protocol)[11] 구조가 RADIUS와 쉽게 결합할 수 있으며, 어떤 링크 계층에서도 동작할 수 있게 준비돼 있다는 것이다. 따라서 사용자 별로 동적으로 키를 만들어 상호 인증을 하게 했으며, 패킷 단위까지도 승인을 받게 준비했다. 또한 802.1x는 단순한 패스워드뿐 아니라, 지문 등의 생채인식이나 스마트 카드 등의 패스워드가 아닌 것까지도 지원하도록 설계돼 있다. EAP를 이용한 인증방법 중 가장 일반적인 방법이 EAP-MD5와 EAP-TLS[12]이며, EAP-TTLS[13]는 현재 draft 상태이다.

EAP-MD5는 사용자 이름 즉 Identity는 Plain text로 전송하고 인증서버에서 전송한 세션넘버에

해당하는 Identifier와 Challenge 값에 자신의 패스워드를 합쳐서 MD5 해쉬 알고리즘으로 해쉬하여 전송한다. 인증서버는 동일한 절차로 자신이 가지고 있는 인증정보를 해쉬하여 비교하여 인증여부를 결정하여 사용자에게 통보하게 된다. 따라서 단방향 인증 및 패스워드 기반 인증으로서의 한계를 가진다. 또한 계층간 연계에 대한 Primitive가 정의되어 있지 않아 Dynamic WEP을 적용할 수 없다.

EAP-TLS는 인증서버와 사용자 사이에 TLS 세션을 맺을 수 있도록 프로토콜을 정의하였다. 따라서 전송되어진 인증서 기반의 상호인증과 사용자 이름 즉 Identity를 보이지 않도록 할 수 있고, 하위 계층으로의 Primitive를 정의하여 dynamic WEP을 가능하게 한다. 그러나 모든 사용자의 단말에 전자인증서를 가져야만 사용할 수 있고, RADIUS 인증서버 중에서는 MS의 IAS, Funk사의 Steel-Belted Radius 정도만이 지원하고 있어 범용성에서 취약점을 가진다.

EAP-TTLS는 EAP-TLS와 같은 mutual Authentication을 제공하고 EAP-TLS가 가진 인증서 관리의 어려움을 해결할 수 있으며 인증 서버는 인증서를 사용하나 사용자는 인증서가 아닌 ID, password 형태의 인증 방식을 사용한다. EAP-TTLS는 서버의 인증서를 이용하여 one way TLS 세션을 만든 후 세션을 통해 사용자의 ID, password 기반의 인증 작업을 마치게 되며 무선 구간에서 사용할 키 생성 및 분배를 실시한다.

III. 무선랜에서의 이동성 보장

1. 모바일 IP의 이동성관리

Mobile IP는 이동노드가 Mobile IP를 통해 이동성을 제공받기 위해서는 여러 단계가 필요하다. 이중에서 가장 먼저 이루어져야 할 과정은 이동노드가 agent들이 보내는 advertisement에 따라 자신의 위치를 판단하고 CoA(Care-of-address)를 획득하는 과정이다. 이 단계를 마친 후에야 이동노드는 자신이 어떤 위치에 있는지를 판단하고 registration request, reply 과정을 통해 home agent와 터널링을 통해 Mobile IP 서비스를 받을 수 있기 때문이다. 이동노드가 home link상에 있을 때는 일반적인 IP 라우팅 동작을 통해 자신의 home IP address를 이용하여 인터넷 등으로 연결할 수 있고 외부 link로 이동하게 되면 CoA 획득, home agent의 등록요청, 등록응답, 터널링의 Mobile IP 절차를 통해 인터넷으로 연결될 수 있다.

경로 최적화란 Correspondent node(CN)에서 이동 노드로의 데이터그램 라우팅의 최적화를 구현하기 위해 기본적인 Mobile IP를 확장한 것이다. 경로 최적화를 하지 않으면 이동 노드를 목적지로 하는 모든 데이터그램은 이동 노드의 홈 에이전트를 거쳐 라우팅 되고, 홈 에이전트는 각각의 데이터그램을 이동 노드의 현재 위치로 터널링 된다. 그리고 이 프로토콜은 CN에게 이동 노드의 위치를 저장할 수 있는 수단을 제공하여 이동 노드로의 직접 전송을 가능하게 한다. 또한 이동 노드가 이동할 때 데이터그램의 손실을 막을 수 있으며, 유효기간이 지난 캐쉬위치(이전 외부 에이전트)에 전송될 패킷을 이동 노드의 현재 위치로 직접 전송되도록 한다.

경로 최적화는 노드에게 하나 이상의 이동 노드의 CoA를 포함하는 바인딩 캐쉬를 유지하는 수단을 제공한다. 이동 노드에 IP 데이터그램을 전송할 때, 전송자가 목적지 이동 노드의 binding cache entry를 가지고 있다면 저장된 mobility binding에 나타나 있는 CoA로 데이터그램을 직접 터널링 한다. 그러나 전송자가 어떠한 binding cache entry도 가지고 있지 않으면 이동 노드를 목적지로 하는 데이터그램은 다른 IP 데이터그램과 마찬가지로 이동 노드의 홈 네트워크로 전송되고, 홈 에이전트에 의해 이동 노드의 현재 CoA로 터널링 된다. [그림 1]은 위에서 설명한 경로 최적화 방법을 도식화 한 것으로 binding cache entry를 관리하기 위한 네 가지 메시지 흐름을 보인다.

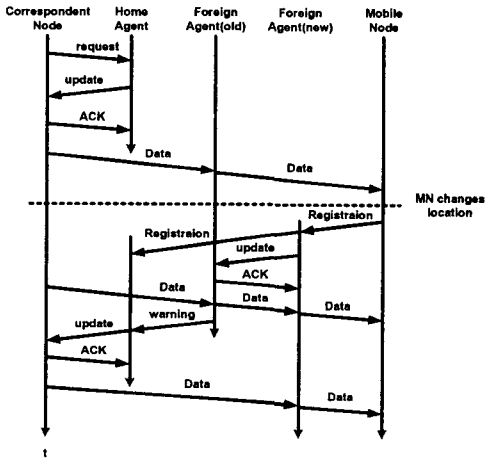

그림 1 최적화된 Mobile IP의 흐름도

2. IAPP (Inter Access-Point Protocol)

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 공유한다. 따라서, 무선단말에서 유연하게 움직이는 로밍 프로토콜은 AP(Access Point) 간의 실시간 정보를 통해 움직이는 단말 장치의 위치가 어디인지 관리해 준다. IEEE 802.11과 IAPP 관계 IAPP 교환 방식은 다음과 같이 AP간에서 실현되고, AP들이 연결된 유선 인프라와 같은 분산 시스템을 통해 이동된다.

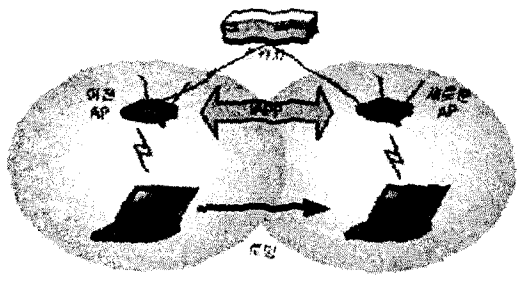

그림 2 IAPP Protocol의 개념

무선단말이 로밍하거나 하나의 AP에서 다른 AP로 이동할 때, 새롭게 로밍할 AP에 대한 재결합은 무선단말이 네트워크 연결을 유지 확인할 때 AP는 무선단말을 인식한다. 그러나 이전의 AP는 무선이동단말에 데이터의 흐름을 건네주지 않기 때문에 이전에 로밍이 끝난 AP는 2가지 다른 방법으로 정보를 얻는다.

▣ 수동적인(passive) 방법: 이동무선단말은 이전 로밍이 끝난 AP의 무선 포트가 아닌 이더넷 포트에서 받은 트래픽을 처리하고 이전 AP의 브리지테이블을 갱신한다.

▣ 능동적인(active) 방법 : 새롭게 로밍할 AP는 이전 로밍이 끝난 AP에게 무선이동단말이 재결합했다는 정보를 주고 이전 AP가 여러 가지 방법을 통해 새로운 AP에게 데이터의 흐름을 건네준다.

IAPP는 위의 2가지 방법으로 구현되며, 능동적인 방법의 IAPP는 다음과 같은 장점이 있다. 브리징 테이블의 갱신 지연이 생기지 않으며 이동무선단말의 로밍이 끝났을 경우, 트래픽 분실이 없고 AP 간의 추가적인 정보를 전달할 수 있다.

3.무선랜에서의 이동성 보장 연구

1) Handover시 MAC 계층에서의 고려

Handover가 발생하는 경우를 구현할 경우 단말에서 어떻게 처리할 것인지에 대해 정확하게 구분할 필요가 있다. 실제 MAC계층에서 발생하는 Association, Reassociation, Disassociation 과정과 상위 IP계층 이상에서 발생하는 사용자 인증 및 접근제어와 분리하여 구현할 필요가 있다. MAC 계층에서 다른 AP로 이동과는 별도로 상위에서 인증이나 접근제어가 이루어지지 않으면 Handover는 이루어지지 않기 때문이다.

다음의 예를 보고 상위 계층에서의 Handover나 로밍에 관해서는 여러 가지 방안들이 다수 있지만 하위 MAC 계층에서의 Handover를 위한 표준은 802.11f IAPP만이 있는 이유를 생각해 보자.

BSSID가 ANY로 설정되어 있는 경우 MAC 계층에서 이동을 설명한다. 우선 단말이 이전 AP에 등록되어 사용 중이다가 새로운 AP의 영역으로 이동했다면 MAC 계층에서 새로운 AP와 자동적으로 Association을 시도할 것이다. 이는 기존 802.11b 모델의 무선랜에서 간단히 구현되어 있는 내용이다. 이와 같이 802.11 MAC 계층에서 AP간 이동이 문제가 없으나 WEP을 사용한 암?복호화의 문제와 인증문제를 해결하기 위해 IAPP를 이용하여 그 문제를 해결한다.

세부적으로 MAC에서 어떻게 처리하는가는 802.11 표준에 정의가 되어있다. 그 부분은 MAC 계층 및 PHY 계층을 관리할 수 있는 관리모델에서 가능하며 대부분의 하드웨어로는 구현되어 있다. 게다가 윈도우 드라이버가 제공되는 경우 NDIS상에서 이러한 MIB(Management Information Base)에 접근이 가능하며 이를 이용해 새로운 AP를 찾고 이동을 위해 Association을 시작하게 할 수 있도록 프로그래밍할 수 있다.

이 방법을 이용하면 단말은 자신이 새로운 AP로 접속을 했는지 알 수 있고 그에 따라 인증 및 접근을 위한 EAPOL-Start를 전송할 수 있는 것이다.

2) Mobile IP와 IAPP의 연동

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 Handover를 적용할 수 있도록 하는데 있다.

[그림 3]에서 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 Handover를 수행한다

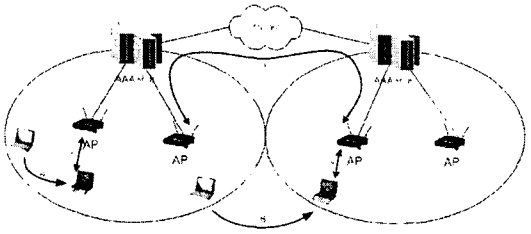

그림 3 Mobile IP와 IAPP의 연동 시나리오

실제로 적용 시에 IAPP에는 사용자 인증단계가 없다는 문제가 있어 보완되지 않는 경우 Mobile IP와 연동하기 어렵다. 즉 이동한 단말이 실제로 이전 AP에서 사용했었는지 또는 그 사용했었던 단말이 현재 단말인지를 확인할 수 없다. 그로 인해 위와 같은 도메인간 이동시에는 Fast Handoff를 수행하기 어렵고 따라서 Seamless Handoff가 가능하지 않다.

앞서 예기했던 이유로 인해 공중 무선랜 네트워크에서 이러한 연동 시나리오를 적용하기에는 힘든 문제가 있다. 이 부분은 단순히 IAPP만을 사용할 수 없음을 얘기하며 단말의 인증이 보안적으로 안전할 경우에 한해서만 이전 AP와의 인증 정보 및 연결정보를 이용하여 Seamless 서비스를 제공할 수 있다는 것을 의미한다. 따라서 단말의 보안적인 인증이 보장되어야 적용이 가능할 것이다.

IV. 이동성이 보장된 AAA 모델검증

1. 제안된 네트워크 모델

본 절에서는 802.1x 기반의 인증 모델 및 접근 제어와 RADIUS Accounting, 그리고 이동성을 지원하기 위한 802.11f의 IAPP를 확장하여 적용된 3가지의 시나리오와 확장된 Mobile IP가 적용된 시나리오를 제안하고 시뮬레이션을 통해서 제안된 모델을 검증한다.

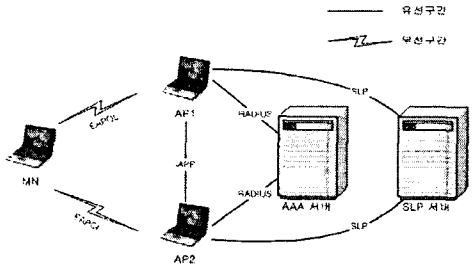

그림 4. AAA 무선 네트워크 모델

[그림 4]는 AAA와 로밍 및 핸드오프를 검증하기 위한 AAA 무선 네트워크 모델로써 본 절에서 설명하는 모든 시나리오에 대한 기본 모델이 된다. 802.1x에 기반을 두었고, 802.1x 측면에서 MN은 Supplicant PAE, AP는 Authentication PAE, 그리고 RADIUS 서버는 Authenticator가 된다. MN와 AP간에는 EAP 프로토콜(사용자를 인증하기 위한 방법으로 MD5 Challenge를 사용한다)을, AP와 RADIUS 서버간에는 RADIUS 프로토콜을 사용한다. 그리고 시나리오 B에서 AP와 SLP 서버간에는 SLP[14](Service Location Protocol) 프로토콜을 사용한다. 또한 AP간의 통신에는 802.11f의 확장된 IAPP 프로토콜을 사용한다.

2. 제안된 모델의 시나리오

무선 네트워크 모델에 대한 시나리오는 로밍 및 핸드오프가 고려되지 않은 AAA 무선 네트워크 모델(시나리오 A), 로밍 및 핸드오프가 고려된 기존의 AAA 무선 네트워크 모델(시나리오 B) 그리고 본 연구에서 제안하는 모델로써 로밍 및 핸드오프가 고려되고 핸드오프 과정에서의 인증 과정으로 단축시켜 성능을 향상시킨 AAA 무선 네트워크 모델(시나리오 C)의 3가지로 나누었다. [표 1]는 각 시나리오의 네트워크 모델에서 지원하는 서비스의 종류를 요약한 것이다.

서비스 종류	시나리오 A	시나리오 B	시나리오 C
802.1x	O	O	O
AAA(인증,권한,과금)	O	O	O
로밍	O	O	O
핸드오프	X	O	O
802.11f(IAPP)	X	△	O
Seamless 서비스	X	X	O

표 1. 지원 가능한 서비스 종류

1) 시나리오 A

시나리오 A는 핸드오프가 고려되지 않은 AAA 무선 네트워크 모델의 경우이다. 이 모델은 802.1x을 기반으로 AAA와 사업자간의 협약으로 로밍 서비스를 지원할 수 있으나, 핸드오프는 지원하지 않는 모델이다. AP1에 association된 MN가 무선랜 서비스를 받기 위해서는 AAA 서버(RADIUS 서버)로부터 사용자 인증 절차(EAP-Request, EAP-Response,RADIUS.Access-Request, RADIUS.Access-Challenge)를 수행하여 네트워크 사용 허가(RADIUS.Access-Accept, EAP-Success)를 받아야 한다. MN가 AP1의 서비스 영역으로부터 벗어나 AP2에서 무선랜 서비스를 받기 위해서는 (EVENT : Handoff) 핸드오프가 지원되지 않기 때문에 먼저 AP1에서 logoff(EAP-Logoff)를 하고 disassociation 후에 다시 AP2에서 association한 후에 AP1에서와 같이 AAA 서버로부터 네트워크 사용을 위한 인증 절차를 수행하여야 한다. [그림 5]은 시나리오 A의 프로토콜 흐름을 나타낸다.

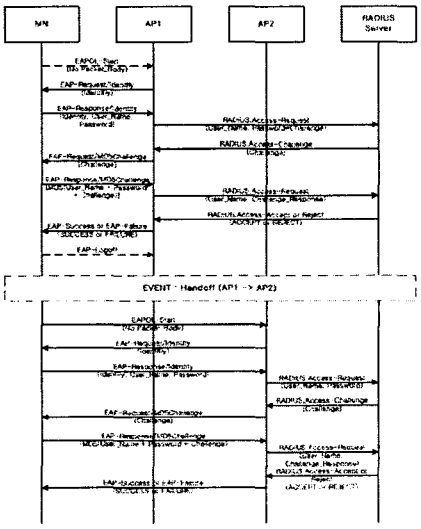

그림 5. 시나리오 A의 프로토콜 흐름

2) 시나리오 B

시나리오 B는 로밍 및 핸드오프가 고려된 AAA 무선 네트워크 모델의 경우이다. 이 네트워크 모델은 802.1x를 기반으로 로밍 및 핸드오프, 그리고 801.11f의 IAPP를 지원한다. 이 모델은 초기에 사용자 인증을 수행하는 과정은 시나리오 A와 같고, 핸드오프가 발생(EVENT : Handoff)했을 때 AP2는 서비스의 위치 정보를 가지고 있는 SLP 서버로부터 AP1의 IP 주소를 얻어와서 (SLP-Service.Request, SLP-Service.Response) MN가 이동했다(IAPP.Move-Notify)고 알려준다. 이로써 MN가는 패킷들에 대한 라우팅 정보가 업데이트 되고, 과금 정보가 전달(IAPP.Move-Response의 Context) 되어 과금 서비스의 연속성이 보장될 수 있다. 그러나 새로운 AP(AP2)에서 서비스를 받으려면 또 다시 RADIUS 서버로부터 인증 과정을 수행해야 한다. 새로운 AP로 핸드오프 할 때마다 매번 사용자를 인증하는 과정은 많은 부하를 가져오기 때문에 seamless 서비스를 보장할 수 없다. [그림 6]은 시나리오 B의 프로토콜 흐름을 나타낸다.

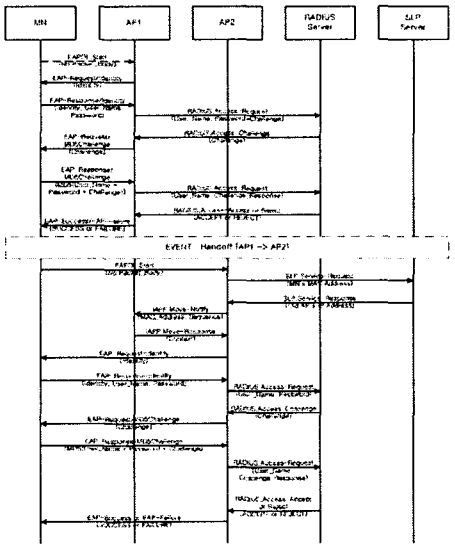

그림 6. 시나리오 B의 프로토콜 흐름

3) 시나리오 C

본 논문에서 제안하고자 하는 인증모델을 구현한 시나리오 C는 시나리오 B에서의 AAA 무선 네트워크를 개선하여 제안한 모델에 관한 것으로

써, 802.1x에 기반 하여 로밍 및 핸드오프를 지원하고, 802.11f의 IAPP에서 인증된 사용자가 핸드오프를 하였을 경우에 AP1에서의 인증 결과를 이용하여 RADIUS 서버로부터의 재인증 과정을 대행함으로써 네트워크 부하를 줄여 seamless 서비스가 가능하도록 한 모델이다. 제안된 모델은 시나리오 B와 비교하였을 때 크게 다른 점은 다음과 같다. (1) 802.11f에 사용된 IAPP의 한계를 극복하고자 인증 기능을 추가하고 2계층에서만 동작하던 부분을 부분적으로 확장하여 일부의 기능을 IP계층으로 확장한다. 이러한 방법을 통해 Seamless 서비스와 이동성을 보장하게 된다. (2) 확장된 IAPP를 이용하면 MN가 핸드오프를 할 때, AP2는 MN가 AP1에서 서비스를 이용하기 위해 인증 받았던 인증정보를 이용하여 MN를 인증함으로써, AAA 서버로부터 재인증 받는 과정에서 발생하는 오버헤드를 줄일 수 있다. (3) MN가 핸드오프를 할 때, MN가 AP2에게 AP1의 IP 주소를 알려줌으로써 AP2가 AP1의 IP주소를 얻기 위해 SLP 서버에 접속하는 과정에서 오는 오버헤드를 줄일 수 있다.

위에서 제시한 차이점은 EAPOL-Start에, 이전 AP1에서 받았던 AP1의 IP 주소와 Authentication Information(MN의 MAC 주소와 랜덤수의 MD5 해쉬값. 여기서는 난수는 초기에 AP1에서 생성된 Identity를 이용하였다.)을 포함하여 전달함으로써 AP2는 이 정보를 바탕으로 AP1으로 통보 확인하여 단말의 빠른 이동문제를 해결할 수 있다. 다음의 [그림 7]은 시나리오 C의 프로토콜 흐름을 나타내고 있다.

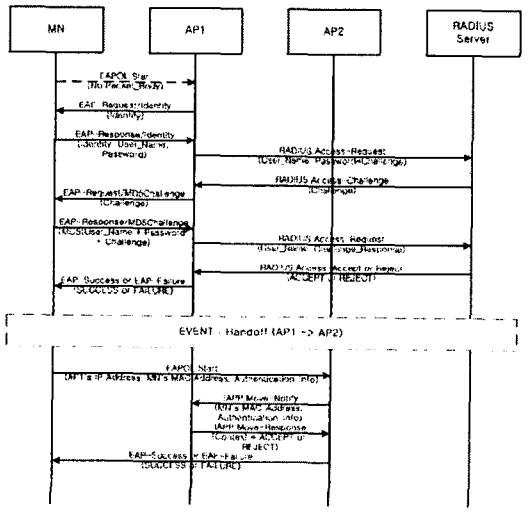

그림 7. 시나리오 C의 프로토콜 흐름

3. 시뮬레이션 검증

1) 프로그램 구성 및 개발 환경

위에서 제시된 3가지의 시나리오 중에 Intra-domain내에서 수행되는 시나리오 A, 시나리오 B, 그리고 시나리오 C에 대해서 시뮬레이션을 수행하고 그 결과를 검증한다. 시뮬레이션 프로그램은 MN, AP1, AP2, RADIUS 서버, 그리고 SLP 서버의 역할을 하는 5개의 프로그램으로 구성되어 있다. 각각의 프로그램은 모두 Microsoft Windows 2000 환경에서 Microsoft Visual C++ 6.0을 사용하여 개발하였다. 다음은 각 프로그램이 하는 역할을 나타낸다.

▣ MN (Mobile Node)

MN는 무선랜 환경에서 AP에 접속하는 역할을 한다. 먼저, AP1에 접속하여 아이디와 패스워드를 입력한 후 AP가 중계하는 RADIUS 서버로부터의 인증 절차를 수행 받는다. 핸드오프 이벤트가 발생하면 AP2에 접속하여 같은 인증 절차의 과정을 수행한다.

▣ AP1 (Access Point 1)

AP1은 처음 MN가 실행되어 접속 요청을 받는 AP이다. AP1은 MN과 RADIUS 서버 사이의 중계를 통해 MN의 인증 절차를 수행하도록 한다. RADIUS 서버로부터 최종적으로 인증결과를 받아 MN의 인증 성공 여부를 결정한다.

▣ AP2 (Access Point 2)

AP2는 AP1에 접속되어 있던 MN의 핸드오프 이벤트가 발생하여 접속되는 AP이다. AP2는 각 시나리오에 따라 MN의 인증절차를 수행한다.

▣ RADIUS 서버

RADIUS 서버는 AP로부터 오는 MN의 인증 요청을 받아 인증과정을 수행하고 그 결과를 통보하는 AAA 서버의 역할을 한다.

▣ SLP 서버

SLP 서버는 AP들의 MAC 주소와 IP 주소 리스트를 가지고 있다. AP2로부터 오는 요청에 들어있는 MAC 주소에 해당하는 IP 주소로 응답한다.

2) 시뮬레이션 블록도

다음 [그림 8]은 시뮬레이션의 블록도이다. 그림

에서 보듯이 각 개체들은 서로 TCP 혹은 UDP 연결을 맺고 EAPOL, IAPP, RADIUS, SLP 프로토콜을 사용하여 데이터를 주고받는다. 다음은 각 개체들간의 연결 정보와 사용하는 프로토콜이다. 괄호 안의 내용은 사용되는 포트번호이다.

▣ TCP : MN와 AP1(1813), MN와 AP2(1815), AP1과 AP2(1816)

▣ UDP : AP1과 RADIUS 서버(1812), AP2와 RADIUS 서버(1812), AP2와 SLP 서버(427)

▣ EAPOL : MN과 AP1, MN과 AP2

▣ IAPP : AP1과 AP2

▣ RADIUS : AP1과 RADIUS 서버, AP2와 RADIUS 서버

▣ SLP : AP2와 SLP 서버

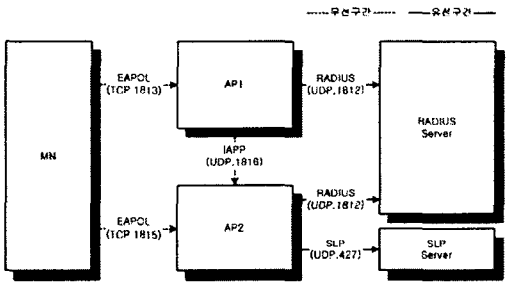

그림 8 시뮬레이션 블럭도

3) 시뮬레이션 결과 분석

제안된 모델의 성능 평가를 위해 각 시나리오별로 20회의 실험을 통해 데이터를 추출하여 평균을 내었다. 그 결과는 [그림 9]과 [그림 10]의 그래프와 같다. 각 그래프의 Y축은 소요된 시간을 나타낸다. 각 그래프의 첫 번째 막대는 각 시나리오의 핸드오프가 일어나기 전, 즉 MN가 AP1에 초기 접속하여 RADIUS 서버로부터 인증 받기까지 걸린 시간을 나타내고, 두 번째 막대는 핸드오프 이벤트가 발생하여 재인증 받기까지 걸린 시간을 나타낸다. 결과 데이터의 비교를 위해서 첫 번째 막대의 수치를 100으로 놓고 두 번째 막대는 그에 대한 비율로 표시하였다.

[그림 9]는 시나리오 B의 결과 그래프이다. 그림에서 보는바와 같이, 핸드오프가 일어나기 전에 RADIUS 서버로부터 인증을 받는 일반적인 절차에서 걸린 시간에 비해 핸드오프로 인해서 재인증을 받는데 걸린 시간이 11% 더 증가되었다. 이것은 AP2가 AP1의 정보(IP 주소)를 얻어오는 과정과 IAPP 프로토콜에 의해서 context를 전송하는 과정에서 오는 오버헤드이다.

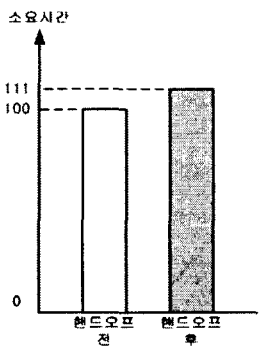

그림 9. 시나리오 B의 결과 그래프

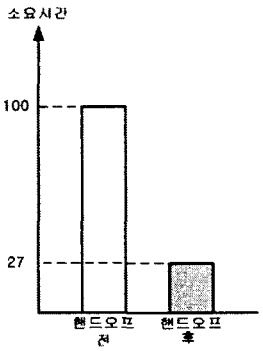

그림 10. 시나리오 C의 결과 그래프

[그림 10]는 본 연구에서 제안하는 시나리오 C의 결과 그래프이다. 그림에서 보듯이, 핸드오프 후의 재인증 과정에서 소요된 시간이 시나리오 B에서 소요되는 시간의 20% 정도로 감소하여 많은 성능 향상을 보인다. 결과적으로, 시나리오 B와 시나리오 C의 재인증 과정을 일반적인 무선랜에서 비교해 보면 본 연구에서 제안한 모델(시나리오 C)이 기존의 모델(시나리오 B)의 성능에 비해 5% 정도 성능이 향상되었음을 볼 수 있다. 이것은 AP1의 정보를 MN가 전달하여 AP2가 AP1의 정보를 얻는 과정에서 오는 오버헤드와 MN에 대한 AP1의 인증 정보를 이용하여 MN를 재인증 과정에서 오는 오버헤드가 줄었기 때문이다.

VI. 결론

본 논문에서는 802.1x와 확장된 IAPP를 이용한 이동성이 보장된 인증 모델을 EAP-MD5 에뮬레이션 프로그램과 확장된 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 논문에서 제안한 모델의 효율성을 확인하였고, IAPP 프로토콜에 인증 기능을 추가하여 AP간의 인증 정보 교환을 통

해 RADIUS 서버로부터의 재 인증 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 정보를 IAPP 프로토콜을 이용하여 전달함으로써 빠른 핸드오프를 지원하고 이동환경에서 실시간 과금에 적용할 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] IP Mobility Support (RFC2002)
[4] IP Mobility Surport for IPV4.revised (RFC3220)
[5] ANSI/IEEE Std 802.11
[6] William A. Arbaugh. "Your 802.11 Wireless Network has No Clothes," March 30, 2001
[7] Fluhrer, Mantin, Shamir "Weaknesses in the Key Scheduling Algorithm of RC4," *Lecture Notes in Computer Science,* August 2001
[8] J.R. Walker. "Unsafe at any key size: an analysis of the WEP encapsulation," *IEEE Document 802.11-00/362,* Oct. 2000.
[9] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications : The Insecurity of 802.11," *Tthe proceedings of the Seventh Annual International Conference on Mobile Computing And Networking.* July,2001
[10] Port-Based network Access Control (IEEE 802.1x-2001)
[11] PPP Extensible Authentication Protocol (RFC2284)
[12] EAP TLS Authentication Protocol (RFC2716)
[13] EAP Tunneled TLS Authentication Protocol (Draft-pppext)
[14] Service Location Protocol(SLP), Version 2 (RFC2608)