무선랜 보안 구조

전북대학교 송창렬
한국전자통신연구원 정병호
전북대학교 조기환*

1. 서 론

인터넷 사용자의 급속한 증가와 무선 통신 기술이 빠른 성장으로, 개인 또는 기업의 사용자는 이동 통신 기술을 이용한 정보의 처리에 따른 이동 전자상거래, 전자 메일, 데이터 전송과 같은 중요한 정보를 비밀리에 전달하고자 하는 보안성 요구가 더더욱 증가하고 있다. 이는 무선매체의 공개성(Openness)에 따른 해킹의 용이성과, 단말의 이동에 따른 보안 체계의 복잡성에 기인한다. 따라서 최근 무선랜 기술 개발과 제품 생산에 있어서 보안성이 가장 중요한 영역으로 자리잡고 있다[1].

IEEE 802.11 무선랜 표준 기술은 기존의 IEEE 802.3 이더넷에 익숙해진 사용자를 중심으로 전 세계적으로 보급되고 있는데, 제 3세대 이동 통신망(IMT2000)의 상용화가 늦어지고 전송률의 한계, 그리고 통신비용의 문제로 인하여 Hot-Spot영역에서 이동 데이터 통신의 수단으로써 무선랜의 인식이 확산되고 있다. 이처럼 무선랜이 이동 통신 수단의 주요 수단이 됨에 따라 정보통신 사업자들은 무선랜의 유선과의 완전한 통합을 지향하게 되었다. 유선랜에서 통신은 이더넷 포트로의 물리적인 접속을 통한 데이터의 전송을 의미한다. 전송되는 데이터는 제 3자가 물리적인 장치를 설치하지 않는 한 비밀성을 보장할 수 있다. 그러나 무선 통신에서 데이터는 전파를 통해 브로드캐스트되기 때문에 일정 범위 안에 있는 모든 무선랜 사용자들은 이를 수신할 수 있게 되어 데이터의 비밀성은 더더욱 중요한 문제가 된다.

무선랜을 통한 네트워크 접속에는 두 개의 보안구간의 정의가 필요하다. 사용자와 AP사이의 무선 구간의 보안과 AP와 인증 서버 사이의 유선 구간의 보안이다. 현재 IEEE 802.11b 표준[2]에서 제공하는 WEP(Wired Equivalent Privacy) 알고리즘을 사용해서 무선 보안이 이루어지고 있으며, 유선 구간에서는 RADIUS(Remote Authentication Dial In User Service)[3]나 TACACS+(Terminal Access Controller Access Control System)[4]프로토콜을 이용하여 인증 정보의 보안성을 제공하고 있다. 그러나 이와 같은 보안 구조에서 문제점이 드러났다. WEP 알고리즘에서는 키 스트림의 단순성으로 인한 실시간 공격과 도청으로 인한 평문의 노출, DoS 공격이 가능하다는 문제점이 있고[5], 클라이언트/서버 프로토콜인 RADIUS는 큰 규모의 적용환경에 취약한 것으로 알려져 있다[6].

본 고에서는 지금까지 무선랜 상에서 사용되는 표준 보안 메커니즘 동향과 이들의 문제점들을 집어보고, 현재 이를 해결하기 위해 진행되고 있는 IEEE 802.1x 프레임워크와 EAP(Extensible Authentication Protocol) 인증 유형, 그리고 Diameter 프로토콜과 같은 최근의 무선랜 보안 방법론을 살펴보려 한다. 2장에서는 현재 가장 널리 사용되는 IEEE 802.11b 표준의 보안 기술과 RADIUS 인증 서버를 이용한 무선랜 시스템의 보안을 살펴보고, 3장에서는 무선랜 보안구조로 IEEE 802에서 표준화되고 있는 IEEE 802.1x에 대해서 설명한다. 4장에서는 EAP 인증의 여러 가지 개발 형태들을 살펴보고, 5장에서는 RADIUS프로토콜의 결점을 보완한 Diameter 프로토콜에 대해서 설명한다. 마지막으로 6장에서는 무선랜 보안 계층 구조를 분석한다.

2. 무선랜 시스템 보안 개요

이동 무선인터넷 기술 중에서 이동성은 적지만 빠른 전송 속도와 높은 대역폭을 가능케 하는 무선랜은

* 정회원

제반 기술의 향상과 장치의 급속한 보급 가운데 전 세계적인 관심의 대상이 되고 있다. 무선랜의 대표적인 기술에는 IEEE를 중심으로 하는 802.11[2]과 유럽의 ETSI(European Telecommunications Standards Institute)를 중심으로 하는 HIPERLAN[7]이 있는데, 본 고에서는 현재 가장 보편화되고 있는 기술인 IEEE 802.11b 기술을 중심으로 무선랜 보안 기술 요소들을 살펴보자.

이동 무선랜을 통해 네트워크에 접근하려는 사용자는 그림 1과 같은 과정의 접속 구조를 갖는다. 이동 사용자(Roaming user)가 자신의 서비스 영역의 근접한 AP(Access Point)에게 서비스 요청을 보내면 AP는 인증 서버(Authentication server)를 이용해 해당 사용자를 인증하고 사용자에게 서비스를 제공한다.

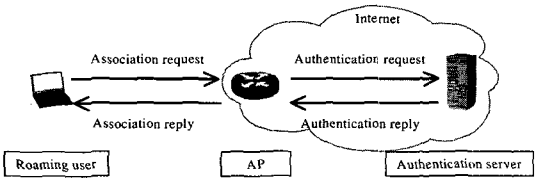

그림 1 무선랜 사용자의 네트워크 접속 과정

2.1 단말과 AP 사이의 보안

현재 널리 보급되어 사용중인 IEEE 802.11b 표준은 무선랜의 인증과 비밀성을 제공하는 두 가지 메커니즘, SSID(Service Set IDentifiers)와 WEP을 정의하고있다[2]. SSID는 무선랜 서브 시스템에서 장비의 네트워크 이름을 지칭하는 것으로써 초보 수준의 접속 제어를 제공한다. 유선랜과 무선 단말을 연결해 주는 장치인 AP(Access Point)는 자신이 주기적으로 보내는 비콘신호에 SSID를 포함하여 브로드캐스트한다. 따라서 SSID를 이용해서 네트워크 접속의 허용/불가를 결정하는 것은 위험하다.

WEP은 IEEE 802.11b는 무선랜 데이터 스트림의 보안성을 제공하기 위하여 정의한 암호화 스킴으로써, 데이터의 암호화와 복호화에 동일키와 알고리즘을 사용하는 대칭형 구조이다. 올바른 WEP키를 소유한 사용자만이 네트워크에 접속하도록 허가하고, 데이터 스트림을 복호화할 수 있도록 하는 접속 제어와 비밀성 보장이 WEP의 사용 목적이다.

IEEE 802.11b 표준에서는 개방 인증 방식(Open system)과 공유키 인증 방식(Shared key system)이라는 두 가지의 인증 형태를 정의하였다. 디폴트 방식인 개방 인증 방식은 전체 인증 과정이 평문으로 이루어지는 방식으로, 단말은 WEP키를 가지고 있지 않아도 AP로의 연결이 가능하다. 공유키 인증 방식에서는 AP가 시도 패킷을 단말에게 보내면 단말은 이를 WEP키로 암호화하여 AP로 응답한다. 만일 단말이 키를 가지고 있지 않거나, 키가 맞지 않으면 인증은 실패하여 연결이 허용되지 않는다.

데이터 기밀성은 WEP을 이용해 제공된다. WEP 알고리즘에서 단말과 AP는 "shared secret"이라고 하는 40비트의 암호키를 공유하고 있다. AP는 단말을 인증하기 위해 random challenge를 보내면, 단말은 40bit의 암호키와 24bit의 IV(Initialization Vector)를 결합하여 이를 RC4 PRNG 암호화 알고리즘에 입력시켜 의사 난수 키 스트림을 생성하고, 이를 이용해 평문을 암호화하여 전송한다. AP는 이를 복호화하여 단말을 인증한다[2].

2.2 AP와 인증 서버 사이의 보안

RADIUS는 NAS(Network Access Server)와 인증 서버사이에 인증, 서비스 허가, 과금에 관한 정보 전달을 위한 프로토콜로써, 유선 환경에서 로밍 PPP(Point to Point Protocol) 사용자를 인증하기 위한 AAA(Authentication, Authorization, Accounting) 프레임워크로 제안되었다[3]. 이는 곳곳에 분산된 NAS를 통하여 서비스에 접속하려는 사용자들을 하나의 데이터 베이스에 통합적이고 효율적으로 관리할 수 있는 이점이 있다. 마찬가지로 무선랜에서도 서비스를 원하는 사용자 수가 증가하고 각 사업자들의 AP가 여기 저기 존재함에 따라 사용자 정보의 통합적인 관리와 사업자들간의 능동적인 정보 교환이 필요하다. RADIUS 서버는 사용자의 연결 요구에 대해 사용자 인증을 해주고, AP는 인증 받은 사용자에게 허가된 서비스를 제공한다.

RADIUS는 다음과 같은 4가지의 특징을 지닌다.

① Client/Server 모델 : NAS는 RADIUS 서버의 클라이언트로 동작하고, 사용자의 정보를 RADIUS 서버에게 전달한다. RADIUS 서버는 사용자 연결 요청을 받으면 사용자를 인증하고 서비스에 필요한 환경 정보를 반환한다.

② Network security : NAS와 RADIUS 서버 사이의 인증은 미리 약속된 shared secret를 통해

서 이루어지고 사용자 패스워드는 암호화된다.

③ 유연한 인증 구조 : 단말은 PPP-PAP(Password Authentication Protocol)나 PPP-CHAP (Challenge Handshake Authentication Protocol), UNIX 로그인과 같은 다양한 방법으로 인증된다.

④ 확장성 있는 프로토콜 구조 : 모든 트랜잭션은 속성(attribute)값에 의해서 이루어지는데, 추가되는 속성은 attribute 필드에 덧붙임으로써 기존의 프로토콜 실행에 방해를 주지 않고 추가할 수 있다.

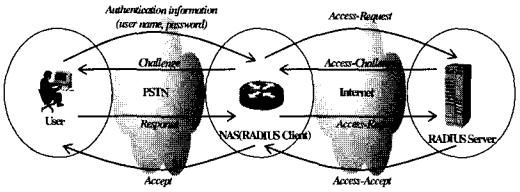

그림 2 RADIUS 동작 과정

그림 2는 RADIUS 동작 과정을 보여준다. RADIUS 서버를 사용하는 사용자는 로그인 프롬프트 상태에서 사용자 이름과 패스워드를 입력하거나, 또는 사용자가 PPP같은 framing 프로토콜을 사용한다면 인증 패킷에 인증정보를 실어 NAS에게 인증정보를 전달한다. 사용자의 인증정보를 받은 NAS는 Access-Request 패킷을 생성하여 RADIUS 서버에게 보낸다. 이때 패스워드는 RSA MD5[8]알고리즘을 사용하여 숨겨진다. 서버는 도착한 패킷의 shared secret이 맞지 않으면 그 패킷을 버린다.

RADIUS 서버는 사용자의 NAI(Network Access Identifier)를 확인하여 데이터베이스에서 사용자의 정보를 찾거나, 해당 인증 서버에게 Access-Request 요청을 보낸다. 만일 Access-Request에 대한 조건이 맞지 않으면 맞으면 Access-Reject로 응답하고, 요청이 적합하면 Access-Challenge로 응답한다. NAS로부터 challenge를 받은 사용자는 알고리즘을 수행하여 NAS에게 응답하고 NAS는 다시 Access-Request를 발생시킨다. 서버는 사용자의 응답을 검사하여 Access-Reject, Access-Accept, 또는 다른 Access-Challenge를 발생할 수 있다. 결과가 올바를 때 Access-Accept 메시지 안에는 서비스 유형에 대한 정보와 NAS가 서비스할 때 필요한 값들 - 예를 들면 서비스 타입이 SLIP(Serial Line Internet Protocol)이나 PPP인 경우 IP 주소, 서브넷 마스크, MTU(Maximum Transmission Unit), 압축방식 등-의 정보가 담겨있다.

2.3 IEEE 802.11b 보안 구조

2.3.1 보안의 취약점

802.11b 표준에서 사용자 인증은 MAC(Media Access Control) 주소를 이용하여 암호화되지 않은 상태로 수행된다. 각 AP는 인가된 단말의 MAC주소 리스트를 가지고 있고 접속을 요청하는 단말의 MAC 주소를 자신의 리스트와 검사하여 유효한 사용자인지를 판별한다. 하지만 이와 같은 MAC 주소 인증 방식에서 누군가 네트워크를 도청하고 있다면 브로드캐스트되는 MAC주소를 금방 알아챌 수 있다. 기존의 무선랜은 보안 문제뿐만 아니라 확장성에도 문제가 있다. 사용자 장치의 MAC 주소는 무선랜의 각 AP에 저장되어 있어야 하는데 이는 관리상의 불편함이 있을 뿐만 아니라, 만일 관리상의 실수가 생긴다면 심각한 보안 사고를 초래할 수 있다[9].

WEP은 원래 유선랜과 같은 수준의 보안성을 제공하고자 의도되었으나 근래 여러 보고서에 의하면 WEP 프로토콜은 크랙이 쉽고 무선 데이터 정보 전송시 위험성이 심각하다고 알려져 있다[5]. WEP 알고리즘은 암호키가 상수이고, IV가 너무 작다. 24bit 길이의 IV는 재사용이 가능해서 동일한 의사 난수 키 스트림(Key Sequence)을 생성시키기 쉽다. 예를 들면 11Mbps의 최대 전송 속도를 가지는 시스템에서는 5시간 이내에 IV를 재사용 하게되고, 실제 통신 상황을 가정해 보아도 24시간 내에 IV를 재 사용하게되어 이를 통한 암호화는 공격에 취약하다. IV의 크기가 작은 점을 이용하여 <IV, 키 스트림>을 저장한 실시간 공격 가능성이 많은 것도 WEP의 단점이다[5][9]. WEP은 선택사항이지만 WECA(Wireless Ethernet Compatibility Alliance)의 Wi-Fi인증을 받기 위해서는 40bit 길이의 키를 지원해야 한다.

2.3.2 향상된 보안 구조

IEEE 802.11 WG(Working Group)i 에서는 802.11의 보안 취약점들을 개선하기 위하여 인증주체 사이의 상호인증과 데이터의 비밀성 보장을 포함하는 향상된 보안 메커니즘을 연구중이다[10].

가. 상호 인증(Mutual Authentication)

기존 802.11b 표준에서는 단방향 인증인 MAC 수준의 단말인증만을 지원하였다. 그러나 인증 주체(사용자, AP, 인증 서버) 사이의 상호 인증을 지원하지 않을 경우, 단말이 서로 다른 도메인을 이동하는 경우에 있어서 이들 사이의 인증 결과를 신뢰할 수 없다. 따라서 802.11 WGi에서는 802.1x 프레임워크를 이용한 상위 계층에서의 사용자 인증을 지원하는 메커니즘과, EAP 캡슐화 프로토콜을 이용한 상호 인증을 지원하는 여러 가지 방안이 제시되고 있다.

나. 비밀성(Privacy)

WEP 프로토콜의 취약점을 보완하기 위하여 IV와 암호키의 길이를 증가시킨 WEP2와 AES(Advanced Encryption Standard) 알고리즘이 제안되었다. WEP2는 WEP과 유사하며 많은 속성들을 그대로 사용하였다. WEP2는 WEP과 마찬가지로 RSA Data Security의 RC4알고리즘으로 암호화를 제공한다. 하지만 전보다 더 큰 MAC 암호화키를 사용하고, 기존의 24bit IV의 크기를 128bit까지 확장하여 실시간 공격에 보완하였다. WEP2는 WEP의 ICV(Integrity Check Value)를 사용한다. 이는 암호학적으로 보았을 때에 안전한 것은 아니어서 데이터 무결성에 취약할 수도 있다. 따라서 사용자는 함께 사용할 다른 암호 메커니즘이 있을 경우에만 WEP2를 사용할 수 있다[10].

AES 알고리즘은 WEP프로토콜의 RC4에 추가하여 WEP 비밀성을 제공하기 위하여 만들어진 선택적인 알고리즘으로써 NIST의 블록암호화 표준이다. AES 암호화 알고리즘은 블록 암호 라인달(Rijndael) 알고리즘을 반복해서 사용한다. 라인달 암호화는 키 길이와 블록의 크기가 가변이다. AES 키는 128, 196 또는 256bit로 구성될 수 있는데 802.11에서는 128bit를 길이의 키로 암호화한다.

3. IEEE 무선랜 보안 프레임워크

IEEE 802 무선랜 기반구조 관리에서 서비스 허가를 얻은 사용자와 올바른 장치에게만 서비스를 제공하는 서비스 제약이 필요하게 되었다. 802.1x란 임의의 사용자가 네트워크에 접근할 때 접근 포트에서부터 인증을 실시하고자 하는 포트 기반 네트워크 접속 제어(Port based Network Access Control) 구조이다[11]. 이는 점대점 연결 특성을 가진 랜 포트에 연결된 인증된 장치에게만 서비스를 제공하기 위해 IEEE 802 무선랜 기반구조의 물리층 접속 특성을 이용한다. 여기서 포트란 랜 기반 구조에 부착되는 단일 접속점으로써 서비스를 제공하거나 받을 수 있는 수단으로써 MAC 브릿지의 포트, 네트워크 인터페이스 카드 등이 있을 수 있다.

3.1 802.1x의 특징

포트 기반 접속 제어의 동작을 기술하는 측면에서 시스템의 포트는 접속 제어 작용에서 두 가지 역할로 구분할 수 있다. 시스템의 서비스를 제공받으려는 Supplicant와 해당 포트로의 접속을 허용하기 전에 인증 절차를 수행하려는 Authenticator이다. Supplicant의 인증을 수행하기 위하여 Authentication Server를 이용하는데 현재 많이 사용되고 있는 Authentication Server는 RADIUS가 있다.

그림 3은 802.1x 포트 기반 네트워크 접속 구성을 보여주고 있다. Supplicant와 Authenticator 사이의 모든 통신은 EAPOL(EAP Over LAN) 캡슐화 형태를 통해 이루어지고, Authenticator와 Authentication Server사이의 통신은 EAP패킷을 RADIUS 프로토콜로 repackage하여 이루어진다.

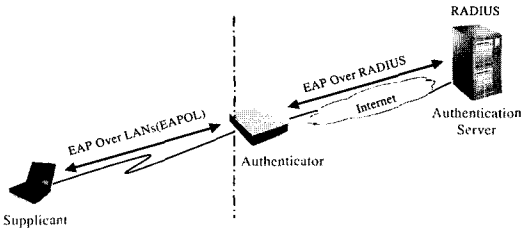

그림 3 무선랜의 포트 기반 네트워크 접속 위상도

3.2 802.1x의 동작 원리

포트 기반 네트워크 접속 제어를 이용하면 랜 접근에 대한 두 개의 구별된 지점을 만들어 내는 효과가 있다. Controlled Port는 포트가 인증 상태에 있을 때에만 PDU(Protocol Data Unit)들의 교환을 허용하고, Uncontrolled Port는 인증 상태에 상관없이 PDU들의 교환을 허용한다. Controlled Port에서는 Authorized와 Unauthorized의 두 가지 상태를 이용하여 PDU들의 흐름을 제어한다.

그림 4는 Authenticator, Supplicant, Authentication Server사이의 관계와 그들 사이의 정보교환을

보여준다. Authenticator System은 Uncontrolled Port를 이용하여 Supplicant System과 Authentication Server System 사이에 인증을 수행하고, 인증에 성공했을 경우에 Controlled Port를 인가하여 서비스를 제공한다. 이와 같이 포트 기반 네트워크 접속 제어는 Controlled Port를 조작함으로써 인증된 사용자만이 서비스에 접속할 수 있도록 하는 인증 메커니즘이다.

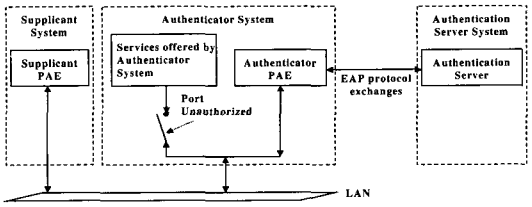

그림 4 Authenticator, Supplicant, Authentication Server의 역할

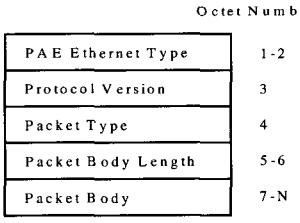

그림 5 802.3/이더넷에 대한 EAPOL 프레임 형태

3.3 패킷 포맷

802.1x는 Supplicant, Authenticator, Authentication Server 사이의 인증 정보 교환수단으로써 EAP[12]를 차용하여 기존 인증 프로토콜의 장점을 취한다. EAP는 다중 인증 메커니즘을 지원하는 일반적인 프로토콜로써 스마트 카드, Kerberos, 공용키 암호화, OTP(OneTime Password)를 포함한 수많은 인증 구조를 지원한다.

802.1x에서는 Supplicant와 Authenticator사이의 패킷 전송을 위하여 EAPOL이라는 캡슐화 기술을 정의하고 있다. 현재까지는 802.3 이더넷 MAC과 토큰링/FDDI MAC을 위한 EAPOL 캡슐화가 정의되어 있는데, 그림 5는 802.3/이더넷에 대한 EAPOL프레임 형태를 보여준다. 프레임은 PAE(Port Access Entity)에 의해서 할당되는 고유의 이더넷 Type값인 PAE Ethernet Type 필드, 지원하는 프로토콜 버전 값인 Protocol Version 필드, 전송되는 패킷의 유형을 표시하는 Packet Type 필드와 패킷의 길이와 내용을 나타내는 Packet Body Length, Packet Body필드로 구성되어 있다.

3.4 프로토콜 동작

그림 6은 서비스 이용자와 서비스 제공자 그리고 인증서버 사이의 포트 기반 네트워크 접속 메커니즘의 과정을 보여준다. 사용자가 네트워크 로그온 다이얼로그 박스에 사용자 이름과 패스워드를 입력하고, 단말과 RADIUS 서버는 상호 인증을 수행한다. 패스워드와 같은 모든 기밀정보들은 모니터링이나 다른 종류의 공격에 대해서 보호되고, 데이터도 암호화되어 전송된다. RADIUS 서버와 단말 사이의 일치되는 키는 현재 로그온 세션동안만 사용이 가능하다.

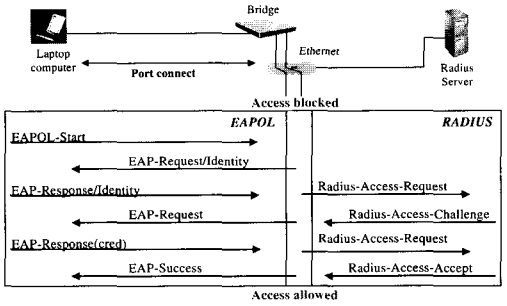

그림 6 802.1x 프레임워크의 접속 과정

프로토콜 동작의 시작은 Supplicant와 Authenticator 양쪽 모두에서 실시 할 수 있는데, Supplicant는 Authenticator 시스템의 포트에 연결할 때에 EAPOL-Start 프레임을 보냄으로써, 또한 Authenticator는 자신의 MAC 포트가 작동 가능할 때 EAP-Request/Identity 프레임을 보냄으로써 인증 교환을 초기화한다. 인증을 시작하기 전에 서비스 접속은 차단되며 프로토콜 교환이 완료된 후 접속이 허가된다.

4. EAP 인증 유형

802.11 WGi에서 새롭게 정의한 ESN(Enhanced Security Network) 프레임워크에서는 안전한 키 분배와 상호 인증 지원을 요구하고 있다. EAP 인증 유형은 이를 위한 방안으로써 여러 무선랜 사업자들은

각각 독자적으로 EAP 인증 유형을 개발하고 있다. 주로 많이 사용되고 있는 EAP 인증 유형은 다음과 같다[9].

① EAP-TLS(Transport Layer Security) : Windows XP에서 802.1x 단말에 사용되는 보안 메커니즘인 EAP-TLS는 사용자의 인증서와 서버의 인증서를 서로 교환함으로써 단말과 네트워크 사이에 인증서 기반의 상호 인증을 제공한다. 그리고 안전한 연결성을 보장하기 위해 사용자 기반, 세션 기반의 동적인 WEP키를 생성하여 분배한다.

② EAP-TTLS(Tunneled TLS Authentication Protocol) : EAP-TTLS는 EAP-TLS의 확장 형태이다. 그러나 EAP-TLS와는 다르게 서버 측 인증서만을 사용하고, 각 무선랜 단말의 인증서 사용을 배제하였다. 또한 기존의 패스워드 프로토콜을 지원하도록 하였으며 사용자 정보는 TLS 프로토콜을 통해 안전하게 터널링 되도록 하였다. 따라서 무선링크를 포함한 RADIUS까지의 전체 네트워크상에서 사용자는 외부 도청자에 대하여 익명성이 보장된다.

③ EAP-AKA(Authentication and Key Agreement) : 3GPP(3rd Generation Partnership Project)에서 제안하여 유럽 3G 이동 통신에서 인증 및 키 일치 메커니즘으로 사용되는 AKA를 적용한 EAP 인증 유형이다.

④ LEAP(Lightweight Extensible Authentication Protocol) : EAP-Cisco Wireless라고도 불리는 이 프로토콜은 시스코 무선랜 AP에 주로 사용된다. 데이터 전송은 동적으로 생성되는 WEP키를 이용해서 암호화되며, 단말과 네트워크간 상호인증을 지원한다.

⑤ EAP-MD5 challenge : 가장 초기의 EAP 인증 유형이고, 유일한 필수(mandatory) 구현 방식이다. 이 프로토콜은 802.1x 프레임워크에서 기본 수준의 EAP를 지원하는 대표적인 EAP 인증 유형이다.

EAP 인증 유형의 표준이 하나로 결정되기 전까지, 앞으로 많은 사업자들이 무선랜 보안 시장에 뛰어들수록 더 많은 EAP 인증 유형들이 생겨날 것이다. 이들 중 IETF TLS 프로토콜을 이용하는 EAP-TLS와 ETSI의 AKA프로토콜을 이용하는 EAP-AKA를 살펴본다.

4.1 EAP-TLS[13]

TLS(Transport Layer Security)[14]는 인터넷에서 통신상의 보안을 제공하는 프로토콜로써 클라이언트 서버간의 어플리케이션에서 도청이나 간섭, 메시지 위조와 같은 비 권한 제어를 방지할 수 있다. EAP-TLS는 TLS 핸드쉐이크를 EAP프로토콜로 확장한 방법으로써 상호 인증과 키 분배에 대한 메커니즘을 포함한다. 그림 7은 EAP-TLS의 핸드쉐이크 과정을 보여주고 있다.

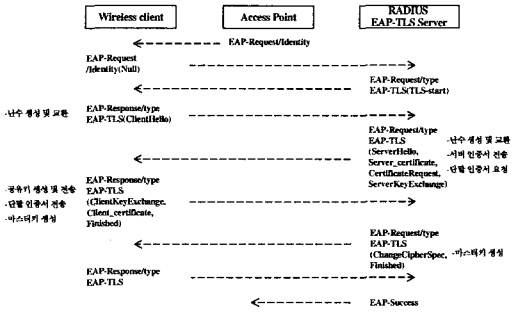

그림 7 EAP-TLS 상호 인증 및 키 분배

무선 단말이 새로운 AP영역에 도달을 감지하게 되면 EAP-TLS(TLS-start)메시지를 통하여 핸드쉐이크가 시작된다. 무선 단말은 난수를 생성하여 ClientHello메시지에 포함시켜 서버로 전송한다. 인증 서버도 난수를 생성하여 ServerHello를 통해 보낸 후, 서버의 인증서를 전송하고, 필요시 단말의 인증서를 요청하는 메시지를 보낸다. 무선 단말은 두 개의 난수와 자신이 생성한 공유키를 이용하여 마스터키를 생성한다. 단말은 서버의 인증서에 포함된 공용키를 이용하여 공유키를 암호화하여 서버에게 전송한다. 서버는 자신이 가지고 있는 비밀키를 이용하여 공유키를 추출하고 두 개의 난수와 함께 마스터키를 생성한다. 무선 단말은 서버의 인증서를 통해 네트워크를 인증하고, 단말의 인증서 요청을 통하여 단말을 인증할 수 있게 되어 상호 인증이 가능하다.

4.2 EAP-AKA[15]

AKA는 3세대 이동 네트워크에서 사용되는 인증 및 키 일치 메커니즘이다. AKA는 시도-응답 메커니즘과 대칭적 암호화를 기반으로 하며, 스마트 카드와 비슷한 장치인 UMTS 사용자 신원 모듈(UMTS

Subscriber Identity Module: USIM)에서 동작한다. AKA는 GSM 인증 메커니즘과의 backward compatibility를 지원하는데, GSM과 비교하여 볼 때, 키 길이가 충분히 길고, 사용자뿐만 아니라 서버의 인증을 제공한다. EAP-AKA는 사용자를 인증하고 세션키를 생성하기 위해서 두 번의 왕복절차(roundtrip)를 사용한다. 네트워크는 AAA 프로토콜을 사용하여 사용자의 AAA 서버와 통신한다.

그림 8은 EAP-AKA의 기본적인 메시지 흐름을 보여준다. 먼저 신원요청/응답 메시지 쌍이 교환된다. 그 다음, 인증서버는 난수와 인증 벡터가 포함된 EAP-요청/USIM-시도 메시지를 보내면 단말은 AUTN을 검증하여 네트워크를 인증한다. 단말은 USIM을 통해 AKA 알고리즘을 실행하여 세션키를 추출하고 EAP-응답/USIM-시도 메시지를 보내는데, 네트워크는 이를 검증함으로써 상호 인증을 수행한다.

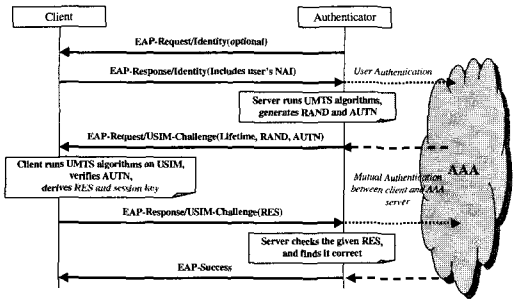

그림 8 EAP-AKA의 시도-응답과정

5. Diameter 프로토콜

RADIUS 프로토콜은 원래 단순한 서버 기반의 인증을 원하는 소수의 엔드유저를 위하여 설계되어, 일단의 소규모 PPP 도메인에서 서버 접속에 대한 AAA 서비스를 제공하는데에 사용되어 왔다. 사용자와 서비스 도메인이 늘어남에 따라 이동이 빈번한 도메인 사이의 이동이 발생하는 환경에서 보안성을 위한 메커니즘의 복잡성과 조밀성이 증가하게 되었다. 따라서 서로 다른 도메인의 이동을 효과적으로 지원하기 위한 peer-to-peer 프로토콜 구조, 브로커 개념의 적용에서 다른 새로운 프로토콜 Diameter의 중요성이 증가하였다.

Diameter는 PPP, 로밍, Mobile IP와 같은 기존 기술과, 새롭게 요구되는 기술에 대한 AAA 서비스를 제공하기 위한 가볍고 확장성이 있는 peer 기반의

표 1 AAA 서비스 요소와 표준기법

네트워크 형태	AAA 서비스 사용자	표준화 기법
고정 네트워크	고정 사용자	RADIUS
	Roaming 사용자	RADIUS 와 Diameter
이동 네트워크	Mobile IP 사용자	Diameter
	Strong Security 사용자	
	Enhanced Accounting 사용자	

AAA프로토콜이다[16]. Diameter는 AVP(Attribute/Value Pair)와 프록시를 지원한다는 점에서 RADIUS와 비슷하나 AVP의 사용 범위에 있어서는 큰 차이를 보인다. RADIUS 주소 공간은 256쌍으로 제한이 있지만 Diameter는 32bit의 AVP 주소 공간으로 갖는데 이는 수백만 쌍 이상을 지원할 수 있다. 이와 같은 강력한 AVP 주소 공간 특성은 이동 사용자나 전용 사용자들을 서비스하기에도 충분하다[17]. Diameter 프로토콜은 서버가 NAS에게 NAS가 처리할 수 있을 만큼의 메시지를 전송하는 것을 허용하는 신뢰성 있는 윈도우 통신 기반의 전송을 지원한다. RADIUS 서버는 사용자가 요구하지 않으면 메시지를 보낼 수 없는 반면 Diameter는 가능하며, 이는 서버가 NAS에게 특별한 과금 기능이나 연결 종료 같은 오퍼레이션 수행을 알릴 때에 유용하게 사용된다. 또한 Diameter는 재전송과 장애 복구 기능을 개선하여 초보적이고 느린 RADIUS에 비해 향상된 망 회복력을 제공한다. 마지막으로, Diameter는 RADIUS가 제공하지 않는 종단간 보안 기법을 제공한다[18].

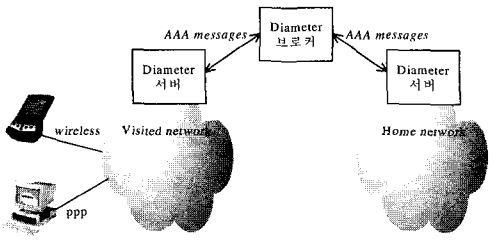

그림 9 로밍을 지원하는 Diameter 구조

Diameter는 로밍과 Mobile IP 망을 지원하기 위해 처음 설계되었다. 그림 9는 Diameter 브로커가 방문망에 접속하여 홈망의 자원을 이용하고자 하는 로밍 및 Mobile IP 사용자에 대해 AAA 서비스를 어떻게 제공하는지를 보여준다. 이 경우 방문망 ISP에 있는

Diameter 서버는 AAA 기능을 수행하기 위해 브로커에 대한 peer로 동작한다.

Diameter 서버와 브로커사이의 통신은 브로커가 CA(Certificate Authority)의 역할을 하므로 안전한 연결상태에서 동작한다. 서버에 대해 인증서를 분배하는 것은 모든 서버가 공유 비밀키를 가지는 것보다도 확장성이 있으면서도 효과적인 방법이다.

Diameter 기본 프로토콜은 그 자체 그대로 사용되기보다 대게 특별한 application을 위해 확장되는 형태로 사용된다. 다음과 같은 IETF WG들에 의해 확대되어 개발되고 있다[19].

① ROAMOPS(Roaming Operations) : ISP들 사이에서 사용자의 로밍을 지원하도록 메커니즘, 절차, 프로토콜을 개발 중에 있다.

② NASREQ(Network Access Server Requirements) : 간단한 다이얼 업 사용에서부터 VPN 지원, 스마트 인증 방법, 로밍에까지 지원하기 위한 NAS의 디자인이 이루어진다.

③ MobileIP(IP Routing for Wireless/Mobile Hosts) : IPv4나 IPv6를 사용하는 IP 노드들이 IP 서브넷과 매체 종류들 사이에 솔기 없는 로밍을 지원하도록 라우팅 기술 개발 중에 있다.

④ AAA : 과금, 전송, 보안, 프록시를 지원하는 Diameter 관련 프로토콜들을 개발하고 있다.

6. 무선랜 보안 계층 구조

데이터의 비밀성 위하여 WEP 알고리즘을 이용하고, 단말의 인증을 위하여 RADIUS 인증 서버를 사용하는 무선랜의 보안은 사용자 수가 많아지고 응용범위가 넓어짐에 따라 여러 가지 문제점에 맞부딪치게 되었다. 현재 이를 위한 각고의 노력이 진행 중에 있으며 그 중 대표적인 802.1x 프레임워크를 이용한 사용자 인증과 EAP 프로토콜을 이용한 상호 인증, 그리고 Diameter 메커니즘을 이용한 사용자 정보와 인증 정보의 관리와 분배를 살펴보았다.

그림 10은 지금까지 살펴본 무선랜을 위한 보안 방법론들의 각각의 역할과 동작하는 계층을 보여주고 있다. 802.11은 링크 계층에서 동작하고 접속 제어와 비밀성을 지원하는 메커니즘이다. 802.1x는 어플리케이션 계층에서 동작하며 사용자의 인증을 수행한다. AAA는 이동 통신 보안 구조로써 어플리케션에서 동작한다. AP간 핸드오프시에는 802.11을 통하여 단말 장치를 인증하고, AP간 프로토콜인 IAPP와 사용자 수준 보안을 제공하는 802.1x를 통하여 단말 사용자를 인증함으로써 근거리 이동시 보안성을 제공하도록 하고 있다. 도메인 또는 서로 다른 기술 사이의 로밍에서는 Mobile IP를 통한 이동성을 제공하도록 표준화가 진행중인데, 802.11 링크 계층 인증과, AAA를 통한 서비스 수준 보안을 제공함으로써 원거리 이동시 보안성 안전을 꾀하고 있다.

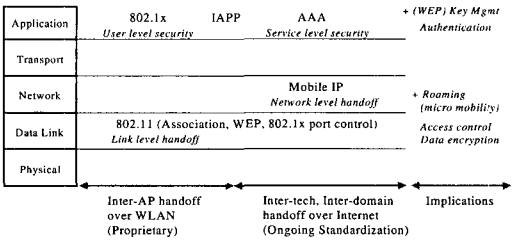

그림 10 IEEE 802.11 계층별 보안 방법론

참고문헌

[1] S. K. Miller, "Facing the challenge of wireless security," Computer.org, pp.16-18, 2001.

[2] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," 1999.

[3] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June 2000.

[4] C. Finscth, "An Access Control Protocol, Sometimes Called TACACS," IETF RFC 1492, July 1993.

[5] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes," University of Maryland, http://www.cs.umd.edu/, Mar. 2001.

[6] Mobile and Wireless Overview, http://www.wheatstone.net/whatwedo/Portal/Standards/radius_diameter.htm

[7] 3G TR 101 031 v2.2.1, "Broadband Radio Access Network(BRAN); HIgh PErformance Radio Local Area Network(HIPERLAN) Type 2; Requirements and architectures for wireless broadband access," ETSI BRAN, Jan. 1999.

[8] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, April 1992.

[9] Secure Authentication, Access Control, and Data Privacy on Wireless LAN, http://www.funk.com/RADIUS/wlan/wlan_solns.asp, Funk software
[10] IEEE802.11-01/018r3, "802.11 TGe Security Baseline Draft Text Rivision 3," IEEE, Mar. 2001.
[11] IEEE Draft P802.1x/D11, "Standard for Port based Network Access Control," IEEE, Mar. 2001.
[12] L. Blunk, "PPP Extensible Authentication Protocol," IETF RFC 2284, Mar. 1998.
[13] D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5," IEEE, 802.11-01/400r22, July 2001.
[14] T. Dierks, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan. 1999.
[15] J. Arkko, "EAP AKA Authentication," IEEE Internet-Draft, draft-arkko-pppext-eap-aka-00.txt, work in progress, May 2001.
[16] P. R. Calhoun, "Diameter Base Protocol," IETF Internet-Draft, draft-ietf-aaa-diameter-08.txt, work in progress, Nov. 2001.
[17] Diameter extends remote authentication, http://www.nwfusion.com/news/tech/0131tech.html#diagram
[18] Christopher Metz, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," Cisco Systems, http://www.computer.org/internet/v3n6/w6onwire.htm
[19] Diameter, http://www.linkionary.com/d/diameter.html

송 창 렬

2001 전북대학교 컴퓨터과학과(이학사)
2001~현재 전북대학교 컴퓨터정보학과(석사과정)
관심분야:무선 인터넷 보안, AAA, 네트워크 보안
E-mail:crsong@dcs.chonbuk.ac.kr

정 병 호

1988 전남대학교 컴퓨터과학과(이학사)
2001~현재 충남대학교 컴퓨터과학과 (박사과정)
1988~2001 국방과학연구소, 선임연구원
2001~현재 한국전자통신연구원 무선 인터넷 보안연구 팀장
관심분야:무선 인터넷 보안, 이동통신, 네트워크 보안
E-mail:cbh@etri.re.kr

조 기 환

1985 전남대학교 계산통계학과 졸업 (학사)
1987 서울대학교 계산통계학과 졸업 (석사)
1996 영국 Newcastle 대학교 전산학과 졸업 (박사)
1987~1997 한국전자통신연구원 선임연구원
1997~1999 목포대학교 컴퓨터과학과 전임강사
1999~현재 전북대학교 전자정보공학부 조교수
관심분야:이동컴퓨팅, 컴퓨터통신, 분산처리시스템
E-mail:ghcho@dcs.chonbuk.ac.kr