主題

802.11b 기반의 무선랜 인증 및 보안 기술

한국전자통신연구원, 이동통신연구소, Global무선LAN 연구팀 박애순, 윤미영, 김영진

차 례

요 약

무선랜 기술은 사설망 내에서의 무선랜 기술을 기반으로 발전해 왔다. 최근 공중망을 기반으로 무선랜 기술이 발전하면서, IEEE 802.11b[1]에서 이루어지던 인증 및 보안 기술로는 안전성을 만족할 수 없게 되었고, 여기에 사용자의 이동성 보장은 필수사항으로 요구되고 있다.

본 논문에서는 지금까지 이루어지던 무선랜 인증 및 보안기술을 사용자의 이동성 보장을 위한 framework으로 발전시키기 위하여 필요한 인증 및 보안기술과, IEEE 802.11b 기반의 무선랜 망에서 필요한 향상된 인증 및 보안기술에 대하여 다양한 관점에서 기술한다. 802.11b 기반으로 이루어지는 보안 및 인증 기술을 보다 향상된 사용자 인증, 데이터 기밀성 향상을 위하여 802.1x[2]기반으로 실현하는 인증기술에 대하여 기술한다. 본 논문의 전개는 이동성을 요구하지 않는 경우의 기본적인 인증 메커니즘인 EAP-MD5[3]기반의challenge/response 메커니즘과, 이동성을 필요로 하는 경우의 인증을 위한 MIP 인증 메커니즘[4-7]에 대하여 기술한다. 마지막으로 사용자의 증가 및 서비스 영역의 확대로 요구되는 새로운 framework에 대하여 기술한다.

1. 개요

인터넷 서비스를 비롯한 다양한 멀티미디어 서비스의 발달과 함께 네트워킹 기술은 다양한 기술을 기반으로 발전해 오고 있다. 현재 급격한 인터넷 서비스의 발달도 급변하는 네트워킹 기술에서 비롯된 결과라 할 수 있다. 특히, 유선망 중심으로 보급되던 서비스가 무선망으로 이동하면서 물리 계층과 MAC 계층의 기술이 보다 향상 되고 또한 상위 계층의 무선 인프라를 위한 다양한 프로토콜들이 등장하고 있다. 다양한 서비스들이 급격한 발달을 이룰 수 있었던 요인 중 하나는 단말기 보급 율의 증가이다. 개인용 컴퓨터는 물론 휴대용 이동 전화의 급격한 증가는 이들 단말기를 위한 서비스 발달을 촉진하는 결과라

볼 수 있다. 이와 함께 인프라 네트워크의 고속화, 초고속 인터넷 접속 기술 등이 발달하였다. 또한 휴대용 단말기들이 보급되면서 사용자 및 단말의 이동성을 위한 서비스는 가장 우선 해결하여야 할 과제로 등장하였고, 이를 위한 많은 노력들이 진행되고 있다. 휴대용 단말이 대중화 되면서 장소에 관계없이 무선 기반으로 통신망에 연결시켜 네트워킹을 이루며 서비스를 받을 수 있는 기술로 무선랜의 보급이 일반화 되고 있다.

무선랜 기술은 미국을 중심으로 진행되고 있는 IEEE 802.11[8] 표준화 기술과 유럽 중심으로 발달되고 있는 HyperLAN2[9-11]의 두 가지 기술로 대별될 수 있다.

이는 Network topology가 변함에 따라 다양한 형태의 네트워크 인프라가 요구되지만, 현재 무선랜 기술의 중심으로 자리 잡고 있는 IEEE 802.11은 미국을 중심으로 발전하고 발전 하고 있고, 요소 기술관점에서 우위에 있는 HyperLAN2는 유럽을 중심으로 자리매김하고 있다. HyperLAN2의 경우 요소 별 기술로 많은 장점이 있으나 비즈니스 모델로 도입하기에는 어려움이 많아, 현재 무선랜은 IEEE 802.11b 중심으로 발전하고 있다.

IEEE 802.11의 표준화는 802.11 WG(Working Group)에서 주관하여 진행하고 그 산하에 역할에 따라 많은 TG(Task Group)로 나뉘어 관련 표준화를 진행하고 있다. 이는 주로 물리 계층과 MAC 계층의 요소 기술 기반으로 분류되어 있으며, 인증 및 암호 관련 기술에 대하여 표준화를 진행하는 복수개의 TG로 분류되어 작업 중에 있다.

본 논문에서는 IEEE 802.11b[1] 기반의 보안 기술 기반의 인증 기술에 대하여, 필요 핵심 요소 기술을 중심으로 전개한다. 802.11기반의 이동 단말(MS: Mobile Station)과 AP(Access Point) 사이에서 수행되던 인증 및 보안 기술이 802.1x framework과 EAP (Extensible Authentication Protocol) 인증의 연계, RADIUS[12]서버나 Diameter[4] 서버와 같은 인증 서버와 통합 연계되어 보안에 대한 강도를 높이고자 하는 해결 구조를 기술하고자 한다.

무선랜에서 이동 단말(이하 MS라 함)에 대한 인증 및 암호는 MS의 이동성 보장에 반드시 필요한 기술이고 MS의 이동은 동일 서브네트워크 내에서의 이동과 서로 다른 서브네트워크 사이에서 이동하는 이동성의 요소 기술로 나눌 수 있다. 다음 [그림 1]에서와 같이 LAN A에 속해있는 AP1에 접속되어 있는 단말이 같은 서브네트워크의 AP2 영역으로 이

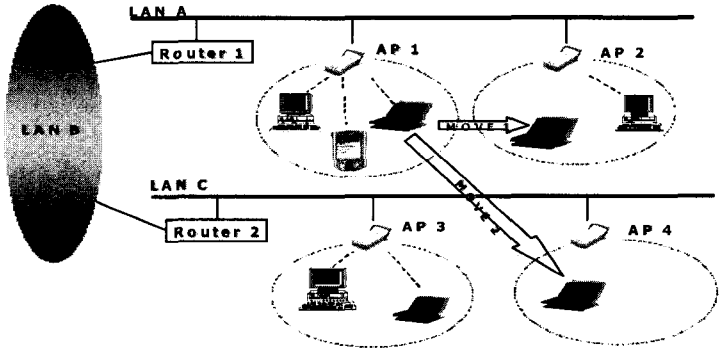

그림 1. 무선랜 망 구성도

동을 한 경우와, 서브네트워크가 다른 LAN C의 AP4 영역으로 이동한 경우로 고려할 수 있다. 이 경우 IP의 이동성이 지원되어야 하는 서비스의 경우와 그렇지 않은 서비스의 경우로 생각할 수 있다. 결국 무선랜에서의 인증 및 암호는 동일 서브네트워크에서 서비스개시 및 이동을 하는 경우, 그리고 서로 다른 서브네트워크 사이를 이동하는 경우 상위의 IP 이동성 프로토콜인 MIP(Mobile IP) 인증 및 암호 기술로 구분된다. 본 논문에서는 이 두 경우를 고려하여 무선랜 망간 연동 시 필요한 인증 및 보안 기술, 정책, 향후 전망 등에 대하여 기술한다.

2. 무선랜 인증 및 보안

■ IEEE 802.11b의 기본적인 접속 제어

802.11에서의 보안 구조는 무선랜에서 MS와 AP사이의 기본적인 접속제어는 SSID(Service Set ID)기반으로 동작한다. SSID는 무선랜에서 논리적으로 영역을 분할하는 의미로 사용하는 번호이고, 보안측면에서는 아주 취약하므로 SSID만을 사용한 접속제어 구조로 무선랜을 구축하는 것은 문제가 있다. SSID를 사용한 접속제어는 처음 접속 시 단말에서 송신한 Probe request에 대한 응답인 Probe response에 실려오거나 또는 AP에서 주기적으로 broadcasting하는 Beacon메시지에 포함되어 있다. 이 메시지 내에 있는 SSID를 이용하여 단말에서 접속 시도를 하고 이를 인지함으로써 기본적인 접속 제어가 일어나게 되고 이 과정이 가장 기본적인 인증 과정이 된다. 여기에 데이터 스트림의 보안성을 위하여 WEP(Wired Privacy Equivalent) 방식의 암호화를 병행하면서 좀더 강도 높은 보안을 제공한다. 그러나 이 방법은 다소의 문제를 안고 있다. 즉, WEP은 동일한 암호키, 복호키 그리고 알고리즘을 단말과 AP가 공유하여 운용하는 방법으로, 동일한 WEP 키를 갖고 있지 않으면 접속하지 못하게 된다. 이 경우 키 분산 시 관리가 어려워지고, 키 공유에도 어려움이 있다. 즉, Static하게 키가 관리되므로 키 분배 적용이 어렵고 보안성이 낮아지는 단점이 있다. 이와 같이 기밀성이나 인증면에서의 문제를 해결하고자 하는 해결방안으로 보다 향상된 보안 기법을 위하여 IEEE 802.11i[13]에서 제안하고 있는 128bit AES(Advanced Encryption Standard)가 있고, 기존의 WEP방식에서 암호화 키 길이를 길게 하여 보안 강도를 높인 WEP2등이 보완책으로 제안되고 있다. 현재 802.11i에서 진행중인 작업은 RSN(Robust Security Network)이라 불리는 보안체계로 802.11 표준을 지원하지 않을 수 도 있는 향상된 기법들이 추가되었다. AP와 MS 양쪽에 모두 향상된 인증 기법이 추가되어 키 관리 알고리즘이 적용되고, 이때 사용되는 데이터 암호화 기법이 앞서 기술한 AES이다. RSN에서는 802.1x port manager, AA(Authentication Agent), AS(Authentication Server)등으로 구성되어 동작된다. 802.1x 위에 AA가 탑재되어 키 관리 및 키 분배, 데이터 인증, 드리고 Replay Attack 방지 등이 가능하게 된다. 802.11i에서 현재 표준화 관련 제안된 알고리즘은 WEP, TKIP (Temporal Key Integrity Privacy), 그리고 AES이다. 이렇게 RSN이 제안되면서 ULA (Upper Layer Authentication) protocol 이 개입되는 구조를 제시하고 있다. 이는 Dynamic Key 할당 및 re-keying 문제 등 기존의 메커니즘에서 제기되었던 문제점에 대한 보완이 가능하고, 중앙의 인증 서버와의 다양한 키 분배 알고리즘을 도입하여 관리한다면 보다 높은 수준의 보안 관리가 가능하게 된다. 이를 위한 802.1X framework 기반의 EAP를 통한 상호 인증 방법을 지원하는 방안이 제안되고 있고, 이는 Mutual Authentication이 가능하면서 기밀성 향상을 위하여 제안된 방안이다. RSN 내의 구성요소 간 관계 구조는 다음 [그림 2]와 같다.

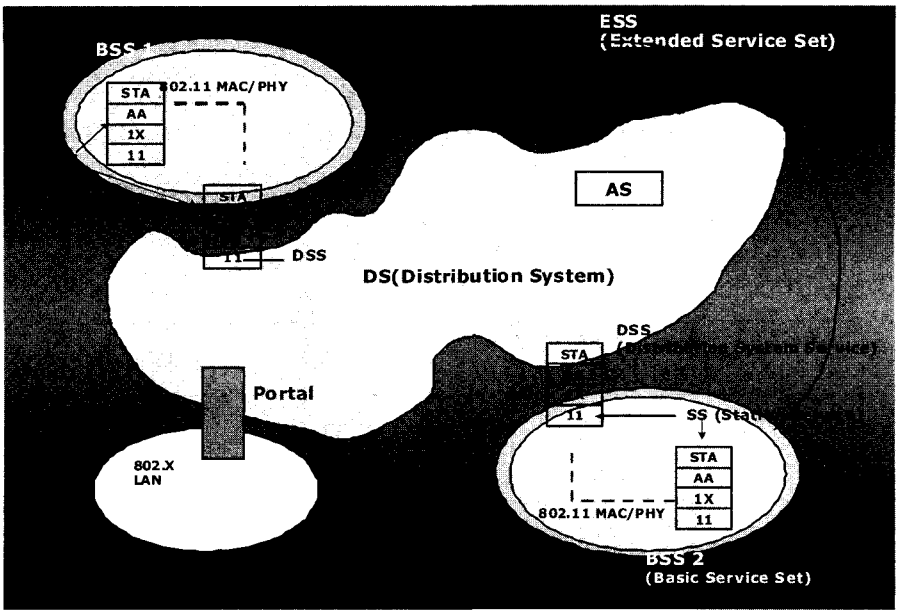

그림 2. 802.11과 802.1x 기반의 네트워크 구성도

무선랜 인증 및 보안은 크게 두 가지 측면에서 고려할 수 있다. 사용자 인증과 데이터 기밀성 보장이다. 무선랜의 인증은 IEEE 802.11에서 제안하고 있는 MAC 인증 및 보안뿐 아니라, 상위 인증 서버와의 연계를 통한 인증 및 보안 방식이 병행으로 수용될 수 있다.

802.11 인증 및 데이터 기밀성 보장은open system 및 shared key방식으로 운용될 수 있고, open system의 경우 단말과 AP사이에 Wi-Fi 표준을 따르지 않는 방식이고, Shared Key 방식은 IEEE 802.11a[14] 또는 802.11b[1] 자체로 키를 보유할 수 도 있고, 상위 인증서버와의 연계를 통한 키 공유도 가능하다. Shared Key의 경우 포트기반의 제어메커니즘인 802.1x기반의 상위 인증프로토콜(EAP-MD5[3], EAP-TTLS[15], EAP-TLS[18], EAP-SRP 등)을 적용한 키 분배 및 키 공유가 가능하다.

■ IEEE 802.1x Framework

802.1x framework 기반의 인증 체계는 RADIUS[12] 서버와의 연계를 통한 사용자 별 인증이 가능하고, EAP와의 연계를 통한 확장성(EAPoL, EAPoW, 등)이 용이하다. EAP는 무선랜 사용자의 안전한 연결을 위해 사용되는 전송 프로토콜이다. EAP-Authentication types에는 EAP-MD5 challenge, EAP-TLS, EAP-TTLS, EAP-SRP등이 있다. 이들은 MS와 인증서버와의 사이에서 이루어지는 인증 체계를 기반으로 장단점을 갖고 있고, 각각의 EAP-Authentication Type 특성은 다음 [표 1]과 같다.

무선랜 가입자의 인증을 위한 802.1x framework 기반 EAP 인증은 RADIUS 서버와의 연계를 통한 EAP-MD5 challenge/response 구조로, 인증 체계를 위한 프로토콜 동작은 다음 [그림 3]과 같다.

표 1. EAP-Authentication Type 별 특성

프로토콜	인증 개요	기타
EAP-TLS	사용자의 인증서(Digital 증명서)와 서버의 인증서(Digital 증명서)를 교환, 인증서 관리하는 곳과 상호 작용을 통해 이루어진다.	- 인증서 기반의 상호 인증 - 사용자 기반, 세션기반의 키분배 지원 - 양방향 인증
EAP-TTLS	사용자의 Password를 이용하고, 서버의 인증서(Digital 증명서) 만을 사용한다. PAP, CHAP등이 사용된다.	- EAP-TLS 확장형태 - 사용자 정보는 TLS를 통해 안전하게 터널링 - 키분배 지원
EAP-SRP	인증서 없이 사용자와 서간에 서로의 패스워드로 동작하며, Password 확인만 가능하다.	- 키 분배 지원
EAP-MD5	사용자의 Password를 서버에서 확인하고, 표준 MD5를 사용한다.	- 가장 초기의 인증 형태 - 키분배 지원 못함. - 단방향 인증

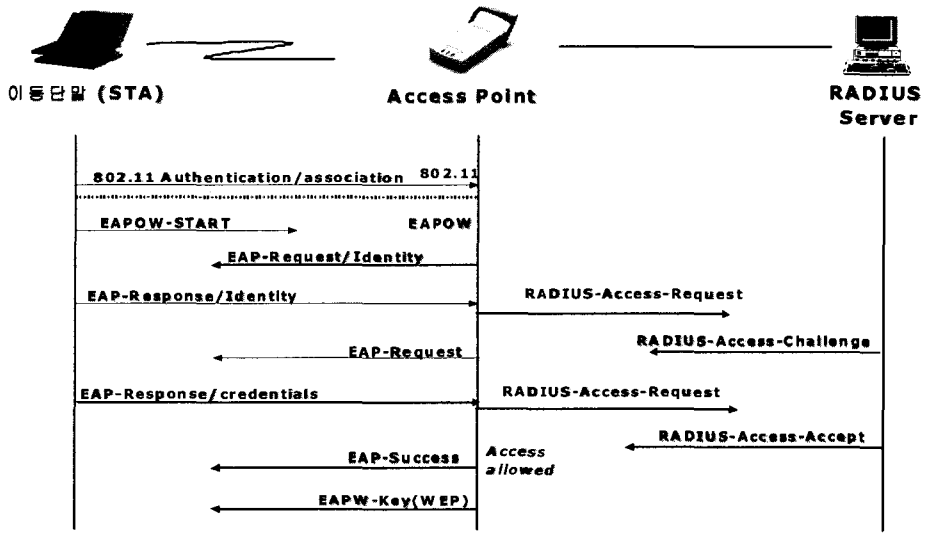

그림 3. 802.1x framework 기반의 EAP 인증 절차

1) MS와 AP 사이에 MAC 레벨 인증 및 암호화를 설정하여 기본적인 접속 절차를 수행한다. (802.11 Authentication, Association)
2) MS에서 네트워크 접속을 시도한다. [EAPoL]
3) AP(Authenticator)에서 접속 요구에 대한 응답으로 identity를 요구한다.
4) MS는 identity를 AP로 보낸다. [EAPoL]
5) AP는 RADIUS 메시지인 Access-Request에 user의 identity를 포함하여 RADIUS server로 전달한다. [RADIUS]
6) RADIUS server는 challenge를 포함한

Access-Request-challenge를 AP로 전달한다. 이 Challenge는 server로부터 요구되는 EAP authentication-type 이다. [RADIUS]

7) AP는 수신한 challenge를 MS로 전달한다. [EAPoL]
8) MS에서 수신한 EAP-authentication-type을 수용할 수 있다면, 이에 대한 응답으로 credential을 보내고, 그렇지 않으면 NOT OK를 보내어 다른 인증 방법을 사용할 것을 요구한다. [EAPoL]
9) AP는 수신한 MS의 응답을 RADIUS server로 전달한다. [RADIUS]
10) MS에서 전송한 credentials이 올바른 것이면 RADIUS server는 해당 MS에 대하여 Access Accept를 생성하고, 그렇지 않으면 Access reject를 생성하게 된다. 생성된 Access-Accept 또는 Reject를 AP로 전달한다. [RADIUS]
11) Authentication이 성공하면 AP는 MS가 네트워크에 접속할 수 있도록 해당 포트를 enabled시킨다.

802.11과 802.1x의 reference model은 [그림 4]와 같이, 802.11 MAC Sub-layer의 상위 계층으로 802.1x가 존재하고, 802.1x는 802.1x SAP을 통하여 인접 계층과 데이터를 송 수신한다.

■ 인증 프로토콜

RADIUS[12]와 Diameter[4]는 대표적인 인증 프로토콜이다. 지금까지 가장 많이 사용되어오던 RADIUS는 client-server 모델로 사용자의 증가나 사용자/터미널의 이동성 보장측면에서 약하다. Diameter는 이를 효과적으로 지원 가능한 프로토콜 구조를 가진 인증 프로토콜로 peer-to-peer 모델을 제시하고 있다.

무선랜의 특성상 사용자의 이동은 필요성이 매우 높다. 이동성은 인증 및 보안 기반으로 제공되어야 하며, 터미널 이동성 보장을 위한 방안으로 제안되고 있는 이동성 프로토콜로 IAPP[16]와 MIP가 있다. MIP의 경우 RADIUS와의 연계를 통한 터미널 이동성 보장에는 기능적으로 많은 제약이 따르므로 Diameter와의 연계 구조를 고려한다. 그러나 기 분포되어 있는 RADIUS 기반의 가입자 수용을 위하여 RADIUS와 Diameter간의 프로토콜 변환 기능을

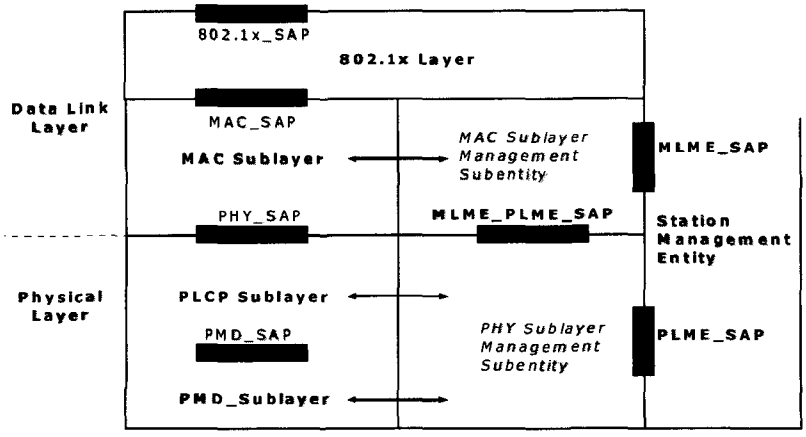

그림 4. 802.1x Reference model

제공한다면, 보다 확장서 있는 망을 구성할 수 있다. 또한 IAPP[16]의 경우 현재 기본적인 인증 연동을 위하여 RADIUS와의 연계를 고려하지만, 추후 서브네트워크 간 이동성 보장 구조와의 연동이나 사용자의 증가, 서브네트워크 영역의 확장 등이 요구된다면 Diameter와의 연계를 고려하여야 할 것으로 예상된다.

■ 이동성 지원 프로토콜

1) IAPP[16]

서로 다른 제조업체에서 생산한 AP 사이의 상호 작용을 보장하기 위함이 주요 기능인 IAPP(Inter Access Point Protocol)는 동일 서브네트워크 내의 서로 다른 AP간에 이동성을 보장하기 위한 프로토콜로, AP간 Layer 2 forwarding 정보 및 AP의 Security Context 정보를 공유함으로써 단말의 신속한 이동을 지원할 수 있는 프로토콜이다. IAPP에서는 MS와 new AP사이에 사용할 WEP 키를 old AP로부터 획득하는 과정에서, 두 AP사이에 ESP(IP Encapsulating Security Payload) [20] 보안 시 사용할 Security 정보를 공유하기 위하여, 인증서버(RADIUS)로 요청하는 구조이다. IAPP 프로토콜구조는 [그림 5]와 같다.

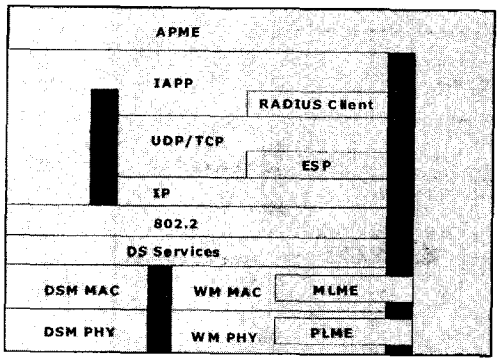

그림 5. IAPP 구조도

APME : IAPP Management Entity, IAPP : Inter Access Point Protocol
ESP : IP Encapsulating Security Payload, DSM MAC, PHY : Distribution System Medium MAC, Physical
WM MAC, PHY: Wireless Medium MAC, Physical

IAPP 프로토콜을 지원하는 동일 서브네트워크에서 AP간에 단말이 이동하는 동작 흐름은 [그림 6]과 같다.

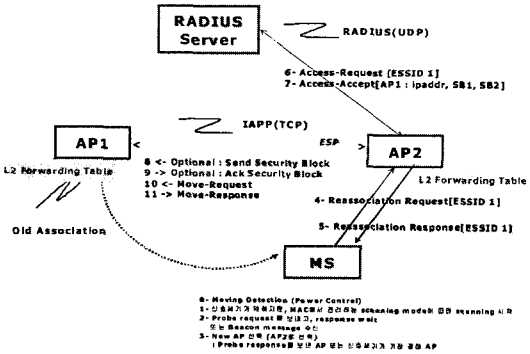

그림 6. IAPP 동작 개요

[그림 6]에서와 같이 MS가 AP1에서 동일 서브네트워크 내의 다른 AP2로 이동 한 경우, MS가 AP2를 선택하는 방법은 두 가지가 있다. Channel Scanning을 통하여 전력세기가 가장 큰 AP를 선정하여 probe request를 보내고 이에 대한 응답으로probe response를 수신하여 Re-association 요구를 하는 경우와, AP에서 주기적으로 브로드케스팅하는 형상 정보를 포함하는 beacon 메시지를 수신하여 해당 파라미터를 참조하여 Re-association을 요구하는 경우이다[1].

이 과정을 거쳐 Re-association을 요구하게 되면, AP2에서는 인증 서버인 RADIUS Server에 Access Request를 보내고 Access Response를 받음으로써 AP2와 AP1에 대한 인가 및 Security 관련 정보를 획득하여 AP1과 AP2 사이에 MS와 사있다.

Security 정보에는 AP2와 AP1사이에 MS가 이동하였음을 통보하고 확인하는 메시지인 Move request와 Move response를 주고 받을 때 이 메

시지를 암호화 및 인증하기 위하여 사용할 알고리즘인 ESP authenticator, AP1으로 설정할 SA관련 SPI 값 등이 포함된다.

2) MIP[17]

동일 서브네트워크 상의 AP간 이동을 위하여 IAPP 프로토콜이 동작된다. IAPP에서는 AP간 fast-handoff를 위하여 AP와 AP사이에 사용될 ESP관련 Security Context정보를 공유하면서, 필요 시 인증 서버로부터 보안 및 인증 관련 정보를 획득하는 구조이다. 그러나 MS가 다른 서브네트워크로 이동을 하게 되면, 상위 IP 이동성 프로토콜인 MIP(Mobile IP)프로토콜을 이용하여 IP간 이동성을 지원할 수 있다.

즉, MS 이동 시 동일 서브네트워크 상의 이동과 다른 서브네트워크로 이동 시 관련되는 이동성 보장 프로토콜이 상이하다. 동일 서브네트워크 또는 서로 다른 서브네트워크 간에 단말의 이동성 보장을 위하여 표준화된 IAPP프로토콜과 MIP 프로토콜이 지원된다면 보다 강화된 인증 및 보안 메커니즘 기반의 이동 서비스를 제공할 수 있을 것이다.

3. 무선랜에서의 IP 이동성 지원을 위한 인증

■ MIP 개요

사용자 및 터미널의 이동성 보장을 위한 기술적 시도는 다방면에서 시도되고 또한 발전되어 왔다. IETF에서 규격을 정의하고 있는 MIP(Mobile IP)는 단말의 IP 이동성 보장을 위한 대표적인 이동성 서비스 프로토콜로, 무선랜 망에서 MS의 이동성 보장을 위한 프로토콜로 정의 할 수 있다. 무선랜 프로토콜에서 이동성을 고려한 서비스 제공 시 기본적으로 MIP를 수용하고, 이에 따른 인증 및 암호 체계가 망의 기반 기술로 동작될 수 있다. 이는 사용자의 위치에 무관하게 인터넷 기반의 끊김 없는 (seamless) 서비스를 가능하게 하는 요소기술로 사용자 인증 및 인가, 그리고 사용료 부과에 대한 과금 기술이 필요함을 의미한다.

무선랜 망에서 사용자의 이동성 제공을 위한 MIP 서비스의 수용 시 일반적인 인터넷 서비스와 공존 가능하고 이들의 인증 및 암호화 체계는 그 범위에 따라 적용 가능 하다. 즉, 일반적인 무선랜에 접속하여 인터넷 서비스를 사용하는 경우, 무선랜 망 사업자의 정의에 의한 보안정책에 따라 기본적인 인증 및 암호가 적용될 수 있고, 이를 서브네트워크간의 서비스 확장으로 연계하기 위하여 AAA 프로토콜과의 연동이 필수 기술로 등장하게 된다. 본 논문에서는 MIP를 위한 구성요소로 MS(MIP 프로토콜내의 표준 서식 표시 시에는 이하 MN으로 표시함), 홈 에이전트(HA), 외부 에이전트 (FA), 그리고 AAA 서버로 구성하고, 인증프로토콜로는Diameter를 기준으로 한다. 이러한 구성에서 MIP 인증을 위하여 MIP 등록 절차에서 일어나는 인증절차, 그리고 암호화를 위한 키 생성 및 분배, 생성 및 분배된 키의 관리 등이 주요 기술이라 할 수 있다.

■ 무선랜에서의 MIP 인증 기반 접속 제어[7]

MIP는 MS와 MS와 HA 사이의 SA(Security Association) 관리가 MIP 인증 및 보안을 위하여 필수적으로 필요한 기능이다. 그러나 MS가 Home-AAA 서버와 SA를 공유할 때에는 MS와 HA 사이뿐 아니라 MS와 현재 서비스를 제공하는 FA와도 SA를 설정할 수 있다. MS를 구분하기 위한 구분자로NAI(Network Access Identifier)를 사용하고, 무선랜에서의 MIP 서비스는 MS의 위치 등록, 등록 해제, 연속등록 등의 과정으로 처리된다.

1) MIP 등록

MS의 서브네트워크 이동 시 절차인 MIP 등록에

서, MS가 HA 및 FA와 SA 설정을 맺지 않은 경우, 보안 및 인증을 위하여 Registration Request 메시지에 MN-FA key request extension, MN-HA key request extension, 그리고 MN-AAA authentication extension을 포함함으로서 Home-AAA 서버에서 MS를 인증할 수 있도록 한다. 이를 수신한 FA는 해당 메시지를 diameter 메시지로 변환하여, MS의 Home-AAA 서버에게 메시지를 전달한다. Home-AAA 서버는 mn-aaa authentication extension으로 MS를 인증하고 또한 MS가 키를 요구한 경우 MS를 위한 키 material 및 이동 에이전트를 위한 키를 생성한다. 생성된 키는 diameter 프로토콜을 통해 홈 에이전트와 외부 에이전트에게 각각 전달된다. key material을 수신한 MS는 홈 에이전트 및 외부 에이전트 간에 사용될 SA를 생성하게 된다. 이는 MN-HA간 혹은 MN-FA간 인증을 위하여 사용된다.

MIP 등록으로 생성된 SA는 lifetime 혹은 MIP key lifetime 동안 유효하다. Lifetime은 MIP 후속 등록 전까지의 시간을 의미하고, MIP key lifetime은 이동 에이전트 및 MS가 사용하는 세션키의 만료 시간을 의미한다. MIP key lifetime은 lifetime과 적어도 일치해야 하므로, 동일한 키를 사용하면서 lifetime을 연장할 수 있다. key lifetime이 만료되기 전에는 AAA를 이용한 연장 등록은 요구되지 않는다.

2) MIP 연속 등록

등록된 세션을 연장하는 경우 혹은 다른 외부 에이전트로 핸드오프 한 경우, 등록된 세션이 Home-AAA서버로 등록하기 위해 MS는 등록 연장 시 Home-AAA NAI[6] 와 HA NAI extension을 첨부하여 registration request 메시지를 생성한다.

3) MIP 등록 해제

세션 해제는 AAA서버가 MS에 할당한 자원을 해제하는 것으로 이동 에이전트들이 세션 해제 메시지

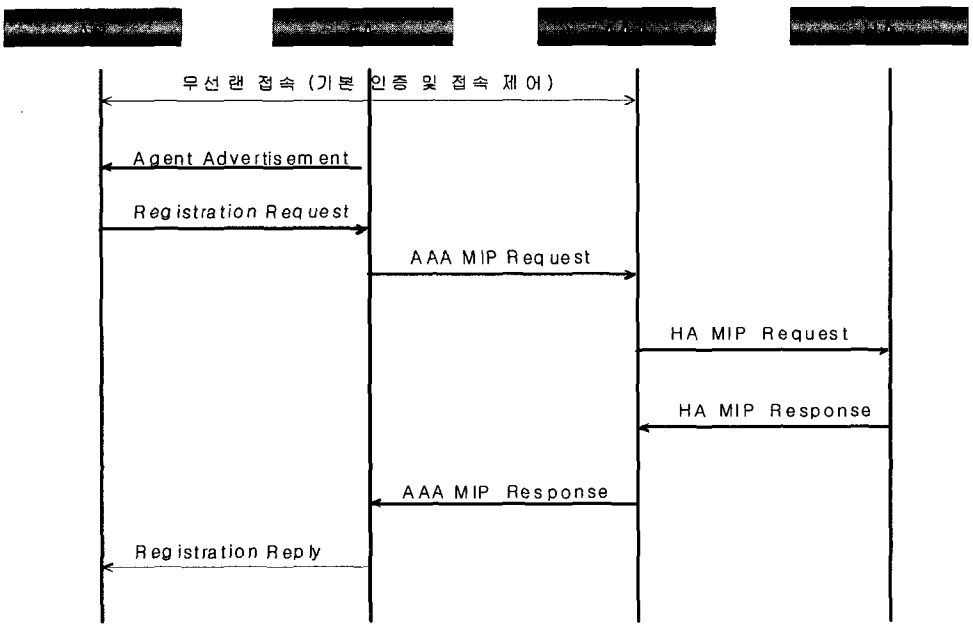

그림 7. Home 망의 자원을 이용하는 경우 MIP등록 절차

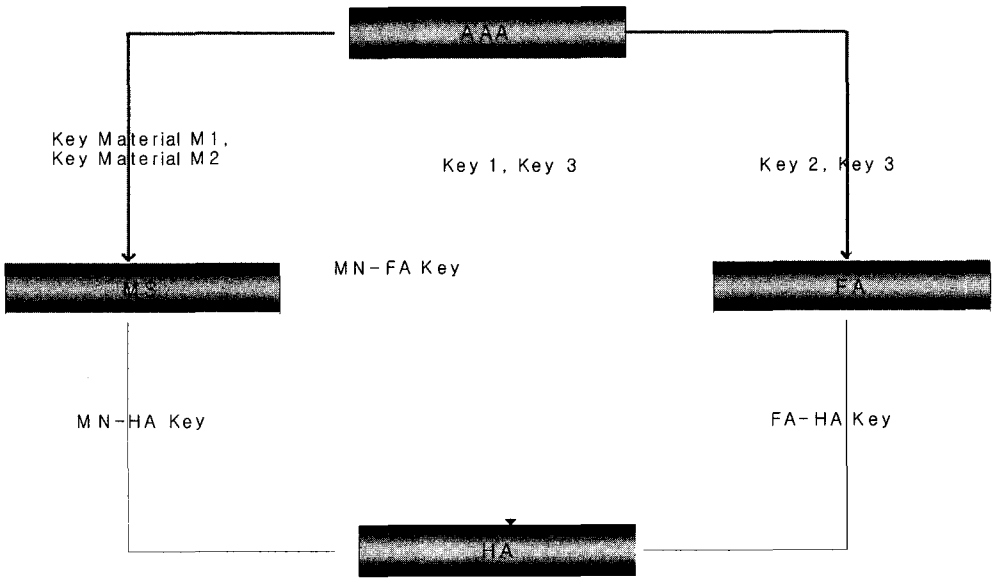

그림 8. MIP 구성 노드 사이의 키 정보 공유 관계

를 전송함으로써 요구한다. Home-AAA 서버는 HA로부터 세션 해제 수신 시에만 해당 노드에 대한 자원을 해제한다. Home-AAA 혹은 Foreign-AAA 서버가 자원 회수를 위한 목적으로 세션 해제를 이동 에이전트들에게 요구할 수 있다.

다음 [그림 7]은 Home 망의 자원을 사용하는 MIP 등록 절차이다.

■ 무선랜의 MIP 인증을 위한 주요 기술[5,7]

1) 키 관리

MS와 이동 에이전트는 Diameter 프로토콜을 통해 획득한 세션 키로 메시지 인증을 한다. MS는 세션키 요구에 대한 응답으로 세션 키를 생성하는데 사용될 64 비트의 key material을 획득하게 되고, 이동 에이전트들은 실제 세션 키를 획득하게 된다. 키 정보 공유관계는 다음 [그림 8]과 같다.

[그림 8]에서와 같이, AAA서버는 MS로 MN-FA 키 생성을 위한 key material M1, MN-HA 키 생성을 위한 key material M2를 분배하고, FA로는 MN-FA 키인 key 1, FA-HA 키인 key 3(128 bit Random Number)를 분배한다. 또한 HA로는 MN-HA 키인 key 2, FA-HA 키인 key 3(128 bit Random Number)를 분배 한다. 이렇게 분배된 키 들은 각 노드에서 관리되어지고 AAA 서버에서 갱신한다. AAA 서버로부터 분배된 정보를 이용하여 MS에서 생성하는 키는 MN-FA, MN-HA 키이고, 한 예로써 MN-FA 키 생성은 다음과 같다.

NN-FA key = HMAC-MD5(key Material M1| Home Address)

2) Authenticator

MIP 사용자의 인증을 위하여 사용되며Mobile IP Agent Advertisement Challenge Extension과Mobile-AAA-Authentication Extension이 있다. 이들 Authentication은 HMAC-MD5를 기본적으로 사용하며 이외의 알고리즘들도 선택적으로 사용될 수 있다. Authenti-

cator 생성은 다음과 같이 수행된다.

Authenticator = HMAC-MD5(preceding Mobile IP data// Type, Subtype, Length, SPI)

이러한 인증 요소들을 사용하여 수행되는 무선랜 망에서의 MIP 인증은 홈망 및 방문망의 HA사용에 따라 다음 [그림 9], [그림 10]과 같은 절차를 갖는다.

■ MIP 인증 및 보안을 위한 핵심 프로토콜

Diameter 프로토콜에서 Diameter 노드(HA, FA, AAA 서버)간 메시지 인증 및 보안을 위해 IPSec 및 TLS를 권고하고 있다. Diameter 에이전트들은 IPSec을 제공할 수 있고, 경우에 따라 TLS를 이용한 암호기능도 제공할 수 있다. 이에 반해 Diameter 서버는 IPSec 및 TLS[20] 모두를 수용하여야한다.

IPSec은 인증과 무결성 및 비밀성 등의 기본적인 서비스를 제공한다. IPSec은 AH(Authentication Header)[19]와 ESP[20] 두 개의 프로토콜을 포함하고 있다. AH 프로토콜은 인증을 담당하는 것으로 기본 IP 헤더와 데이터 및 식별정보에 대한 해쉬값을 포함하는 추가적인 헤더정보를 생성하며, 여기에 포함되는 해쉬는 헤더정보의 무결성을 보장한다. ESP 프로토콜은 인증, 무결성 및 비밀성을 보증하는 프로토콜로 Payload에 대한 인증과 암호화를 수행한다. ESP에 사용되는 암호화 알고리즘은 DES가 기본적으로 사용되며 사용자에 의해 선택이 가능하다. IPSec은 미리 공유된 키를 이용하여 상대를 인증 할 수도 있고, IKE를 이용한 공개 키 암호화 방법을 이용하며 상대를 인증할 수 도 있다. IPSec은 트랜스포트 암호화 모드와 터널 암호화 모드 모두 지원한다. 트랜스포트 모드는 각 패킷의 Payload만을 암호화하고 헤더정보는 그대로 두며, 터널모드는 헤더와 payload 둘 다 암호화 한다.

Diameter 노드간 인증 및 보안을 위해 IPSec 및 TLS를 사용하는 경우 노드간 보안만을 제공하게 된다. Diameter 는 peer 구간 중간에 proxy agent등이 존재할 수 있어, 실제 peer 간 보안은 IPSec 및 TLS로 부족하다. 응용 계층의 end-to-end 보안을 제공하기 위한 방안으로 제시된 것이 CMS application[21]이다. CMS는 인증 및 무결성을 제공하는 디지털 서명과 암호키를 이용한 암호화 서비스를 제공한다. 특히 CMS에서 제공하는 암호화는 Diameter 키 분배시 키를 안전하게 전달하기 위해 사용될 수 있다.

4. 결론

현재 인터넷 서비스를 기본으로 하는 다양한 패킷 서비스들은 다양한 인프라 망을 기반으로 다방면에서 발전을 보이고 있다. 단말 기술의 발전 및 보급률 향성 그리고 다양한 서비스의 발달은 무선랜 망 기술을 발전시키는 주요 요인으로 대두되고 있다. 무선랜은 현재의 서비스 범주에서 더욱 다양한 망의 수용 및 연동을 통하여 인터넷 서비스의 근간망으로 발전할 가능성도 현재로써는 배제 할 수 없다. 기존의 IEEE 802.11 기반으로 운용되던 인증 및 보안 메커니즘이 802.1x 기반의 EAP framework으로 진행되면서 융통성 있는 보완 메커니즘으로 인식되고 있다. 결국 가장 문제가 되었던 static key 관리 등이 해결되면서 가입자 별 인증키 분배 및 동적 키 분배가 가능하여졌고, 중앙에서 집중 관리하면서 관리체계가 더욱 안정화 되었다. 무엇보다도 EAP Framework으로 진화하면서 TLS, TTLS, MD5, IKE등 IETF에서 규정하는 표준화된 다양한 프로토콜들을 상위 인증 및 보안 프로토콜로 채택할 수 있게 되었다. 무선랜에서의 보안 및 인증을 위한 또 다른 노력으로 현재 802.11 WG 산하의

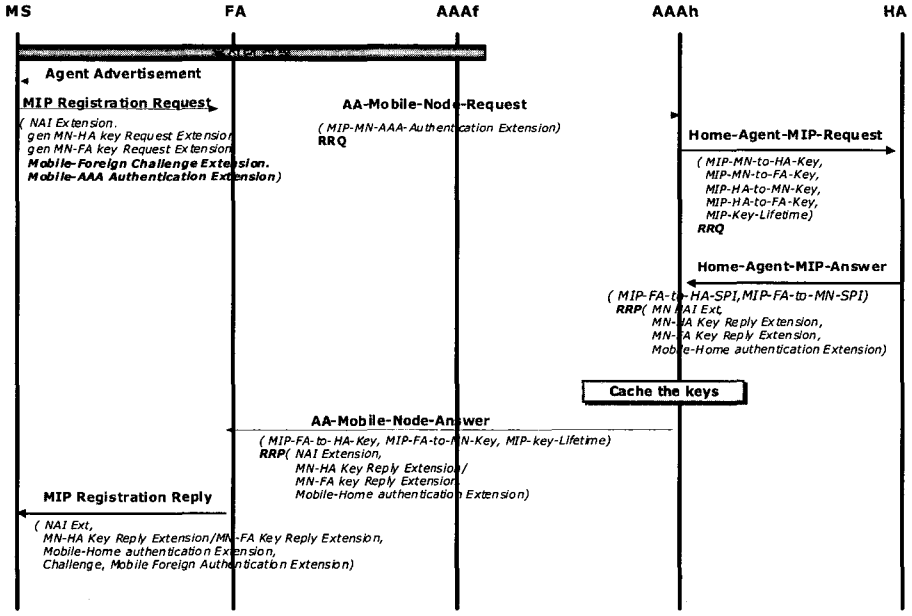

그림 9. 홈망의 자원을 사용하는 경우 MIP 등록에서의 인증 절차

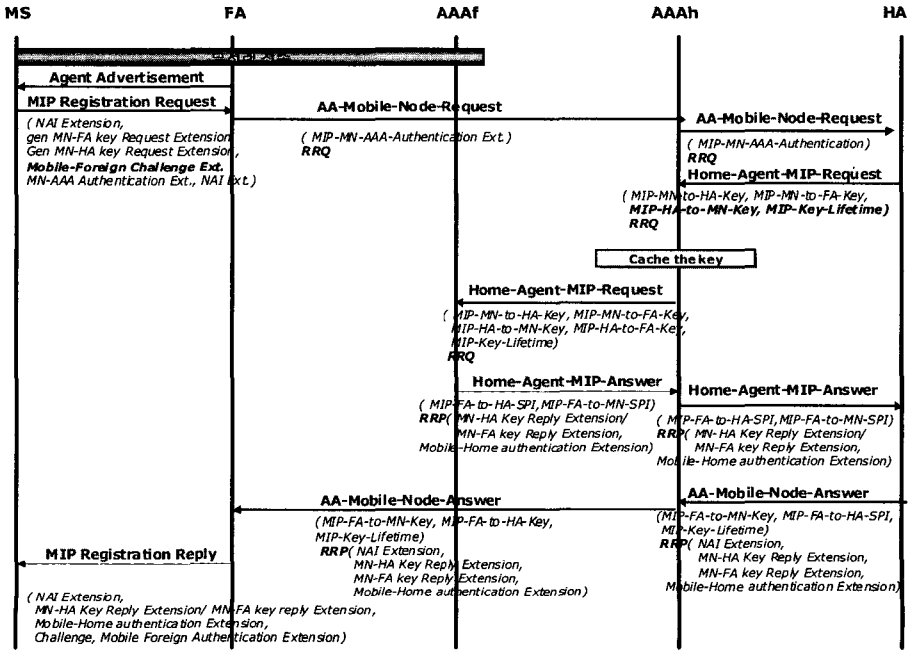

그림 10. 방문망의 자원을 사용하는 경우 MIP 등록에서의 인증 절차

TGi[13]에서 보다 향상된 체계의 인증 메커니즘을 도입하면서 IETF에서 정의하는 다양한 인증 프로토콜 및 암호화 메커니즘들을 연계하여 안전하고 융통성 있는 인증 체계를 구축하고자 하는 노력을 하고 있다. 앞서 기술한 802.1x기반의 EAP Framework 연계에 대한 여지도 충분히 논의되고 있다.

무선랜 망에서 또 하나의 중요한 과제로 서비스 네트워크 간 이동성 지원을 위한 IP 이동성 기술 수용 등이 주요한 관심사로 등장하고 있다. 해결하여야 할 가장 중요한 과제는 망 간 연동시 요구되는 가입자 인증 및 이들에 대한 보안 서비스이다. 서브네트워크 사이를 이동하게 되면 무엇보다도 인가된 사용자에 대한 확인 및 사용자의 권한 검증, 메시지 기밀성, 보안 강화 등이 중요한 위치를 차지하게 된다.

무선랜을 기반으로 하는 다양한 서비스의 발달은 사용자 및 단말의 이동성 보장을 전제로 하여 인증 및 보안 서비스가 보장되어야 하고, 이러한 체계에서 무선랜 기반의 서비스는 많은 발전을 이룰 것이라 사료된다.

참고문헌

[1] IEEE 802.11b, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", 1999

[2] IEEE 802.1X, "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control", 2001

[3] draft-ietf-pppext-rfc2284bis-05, "Extensible Authentication Protocol (EAP)", July 2002

[4] draft-ietf-aaa-diameter-12, "Diameter Base Protocol", July 2002

[5] draft-ietf-mobileip-aaa-key-09, "AAA Registration Keys for Mobile IP", Feb. 2002

[6] draft-ietf-mobileip-aaa-nai-00, "AAA NAI for Mobile IPv4 Extension", April. 2002

[7] draft-ietf-aaa-diameter-mobileip-11, "Diameter Mobile IPv4 Application", June 2002

[8] IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", 1999

[9] ETSI TR 101 031, "HIPERLAN/2: Requirements and architectures for wireless broadband access", Jan. 1999

[10] ETSI TR 101 683, "HIPERLAN/2: System Overview", Feb. 2000

[11] ETSI TR 101 975, "HIPERLAN/2: Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular systems", Aug. 2001

[12] RFC 2865, "Remote Authentication Dial In User Service (RADIUS)", June. 2000

[13] IEEE 802.11i-D2.0, "Draft - Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security", March. 2002

[14] IEEE 802.11a, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High- speed Physical Layer in the 5 GHz Band", 1999

[15] draft-ietf-pppext-eap-ttls-01, "EAP

Tunneled TLS Authentication Protocol (EAP-TTLS)", Feb. 2002
[16] IEEE 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", April. 2002
[17] RFC 3220, "IP Mobility Support for IPv4", Jan. 2002
[18] RFC 2716, "PPP EAP TLS Authentication Protocol", Jan. 2002
[19] RFC 2402, "IP Authentication Header", Nov. 1998
[20] RFC 2406, "IP Encapsulating Security Payload (ESP)", Nov. 1998
[21] draft-ietf-aaa-diameter-cms-sec-04, "Diameter CMS Security Application", March 2002

박 애 순

1987 충남대학교 계산통계학과 학사 1997 충남대학교 전자공학과 석사 2001 충남대학교 컴퓨터과학과 박사 1988~현재 한국전자통신연구원 Global무선LAN 연구팀 선임연구원

관심분야: Mobile 프로토콜, Mobile Security, 이동단말기술, 무선LAN, 망관리

윤 미 영

1999 충남대학교 컴퓨터과학과 학사 2001 충남대학교 컴퓨터과학 석사 2001~현재 한국전자통신연구원 Global 무선LAN연구팀 연구원

관심분야: Mobile QoS , 인터넷 QoS, 무선LAN, Traffic Analysis

김 영 진

1981 고려대학교 전자공학과 학사 1983 고려대학교 전자공학과 석사 1989~1991 벨기에 BTM 방문연구원 1983~현재 한국전자통신연구원 Global무선LAN 연구팀장,

관심분야: CDMA 시스템, IMT-2000 시스템, IP기반 이동통신 시스템, 무선LAN