AP 사이의 상호 운영에 관한 연구

박 미 애*, 김 용 희**, 이 옥 연***

Study on Inter-Access-Point Protocol Supporting IEEE 802.11 Operation

Mi-ae Park, Yong-hee Kim, Ok-Yeon Lee

요 약

무선 인터넷 시장이 커짐에 따라 가장 크게 대두되는 이슈 중에 하나는 802.11 ESS에서의 AP간의 상호 운영과 STA 정보의 안전한 핸드오프이다. IAPP는 액서스 포인트 AP(Access-Ponit)에 다양한 로컬 이벤트가 일어날 때 다른 AP들과 통신하기 위하여 AP 관리 개체에 의해 사용되는 통신 프로토콜이다. IAPP의 기능은 ESS의 생성과 유지를 용이하게 하고, STA의 안전하고 빠른 이동성을 지원하며 AP가 주어진 시간에 각 STA와 단독 결합 요청을 수행할 수 있도록 지원한다. 본 논문에서는 현재 802.11F에서 진행 중인 IAPP의 내용을 중심으로 RADIUS를 바탕으로 하는 IAPP의 운영에 대해서 연구했다.

Ⅰ. 서 론

802.11 네트워크의 기본 구성 블록은 BSS이다. 이것은 이동 가능한 단말(STA)과 이 단말들의 접속 장치인 AP로 구성된다. 하지만 하나의 BSS는 큰 영역을 커버할 수 없다. 따라서 802.11은 BSS를 연결한 임의적인 규모의 무선 네트워크 ESS를 허용하고 있다. BSS의 모임인 ESS는 하나의 BSS에서 다른 BSS로 이동하는 것을 허가한다. 이러한 이동은 AP를 통해 이루어지며 ESS의 구성은 ISO/IEC 8802-11:1990에서 서술된 것처럼 MLME-START.request (BSSType=Infrastructure)를 통한 첫 번째 AP의 초기화로 설정된다. 그리고 다음 AP를 공통 DS(Distribution System)에 의해 상호연결 되도록 하여 가장 먼저 만들어진 ESS를 확장하고 동일한 SSID를 사용하도록 한다. ESS의 AP 멤버들을 정하기 위해 중앙 RADIUS 레지스터를 사용한다.

그림 1은 ESS 구조를 나타낸 것이다.

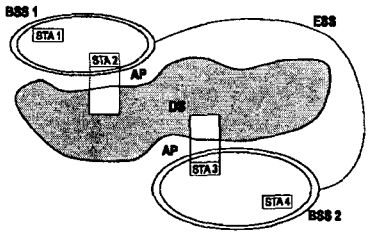

그림 1. ESS 구조

* 국민대학교 수학과 박사과정 (miae34@hanmail.net)
** 광운대학교 수학과 석사과정 (dragon-61@hanmail.net)
*** 국민대학교 수학과 교수 (oyyi@kookmin.ac.kr)

AP는 유선망에서 무선으로 전환하는 장치로 이동하는 STA와 결합하는 유선 허브기능, 브릿지 기능, 홈 게이트 웨이 기능등 다양한 기능을 갖는다. 또한 AP는 DS 서비스를 제공하기 때문에 DS의 기능도 지원한다. 따라서 모든 데이터는 AP를 통해 DS와 BSS사이를 이동하게 된다.

AP는 그림 2와 같이 구성된다.

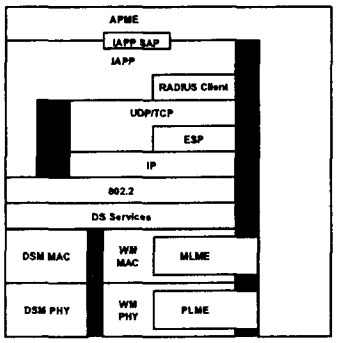

그림 2. IAPP를 포함한 AP의 구조

APME(Access Point Management Entity)는 AP가 가지고 있는 특징과 알고리즘 구현과 802.11의 SME(Station Management Entity)와의 결합을 관리하는 AP의 주요 운영 개체이다.

SAP(Service Access Point)는 APME가 IAPP 서비스를 불러내는 것을 허가하고 단독 ESS 안에 다른 AP에 IAPP서비스 시작의 지시를 수신한다. SAP는 4가지 서비스(요청, 확인, 지시, 응답)를 지원한다. RADIUS 지원을 포함하기 때문에 AP내에 RADIUS 클라이언트가 존재한다.

IAPP 개체는 SAP를 통해 APME에 접근하고 APME가 RADIUS 서버나 DS 안에 있는 AP들과 통신하거나 기능을 수행하기 위해 IAPP 프로토콜을 이용하도록 허가한다. BSSID를 가진 AP가 있을 때 ESS안에 다른 AP의 IP주소를 찾고 IAPP 패킷의 내용을 보호하기 위한 안전한 정보를 얻기 위해 RADIUS 서버를 찾는데 사용된다. 즉, IAPP 개체는 IAPP의 정확하고 안전한 운영을 위해 RADIUS 프로토콜에 의존한다.

IAPP(Inter-Access Point Protocol)란 ESS 안에 있는 STA의 로밍과 AP들의 상호운영을 지원하는 프로토콜로서 AP사이에서 메시지와 데이터를 교환하고 STA 정보의 안전한 핸드오프 메커니즘을 제공한다. IAPP를 사용하는 네트워크 장비는 802.11 AP이고 IAPP의 운영에 작용하는 네트워크 안에 다른 장비는 bridge와 switch와 같은 layer 2 네트워크 장비이다. IAPP 프로토콜은 내부 AP통신을 위해서 TCP를 사용하고 IEEE 802.11f에서 권고된 RADIUS서버와의 요청/응답 교환을 위해 UDP를 사용한다. 또한 layer 2 장비의 포워딩 테이블을 업데이트 하기 위해 layer 2 프레임을 사용한다. IAPP는 3가지 프로토콜을 지원한다.

첫째는 STA가 802.11 결합 요청 프레임을 사용하여 AP와 결합할 때 APME가 MLME로부터 MLME-ASSOCIATE.indication을 수신한 후에 IAPP-ADD.request를 발행하고 이것을 수신한 IAPP 개체는 다음과 같은 작용을 수행한다.

1) IAPP 개체는 DS로 layer 2 업데이트 프레임을 전송한다. 이것은 layer 2 장비로 수신될 이후의 모든 트래픽이 정해진 포트로 전송되기 위하여 layer 2 장비 안에 있는 포워딩 테이블을 업데이트 할 수 있도록 주소화 한다.

2) IAPP 개체는 AP와 STA사이에 결합했다는 것을 DS의 로컬 멀티 도메인 안에 있는 AP들에게 통지하기 위하여 IAPP IP 멀티 캐스트 주소(224.0.1.178)로 IAPP ADD-notify 패킷을 보낸다. 이것은 STA가 새로운 결합을 했기 때문에 이것을 위한 저장 개체를 비워야 한다는 것을 지시한다.

둘째는 APME가 AP와 재결합된 STA를 지시하는 MLME로부터 MLME-REASSOCIATE.indication을 수신한 후에 IAPP-MOVE.request를 발행하고 이것을 수신한 IAPP 개체는 다음과 같은 작용을 수행한다.

1) AP와 통신하는데 필요한 보안 정보와 재결합 요청 안에 나타난 old BSSID로 식별된 AP의 DSM layer 3 주소를 결정한다.

2) 재결합을 요청한 STA의 환경 정보를 저장하고 있는 old AP에 IAPP MOVE-notify 패킷을 보낸다.

셋째는 CACHE를 사용하게 될 때 STA가 AP와 결합하거나 재결합했다는 지시로 APME가 MLME로부터 MLME-ASSOCIATE.indication 이나 MLME-REASSOCIATE.indication을 수신하면 IAPP-CACHE-NOTIFY.request를 발행하고 이것을 수신한 IAPP 개체는 STA의 환경을 요청하는 이웃하는 각 AP에게 IAPP CACHE-NOTIFY 패킷을 송신한다. 이것은 APME가 STA의 환경이 바뀔 때마다 발행하고 STA의 빠른 로밍을 위한 것이다.

그림 3은 IAPP를 나타낸 것이다.

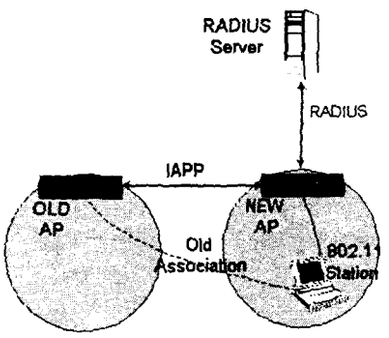

그림 3. IAPP

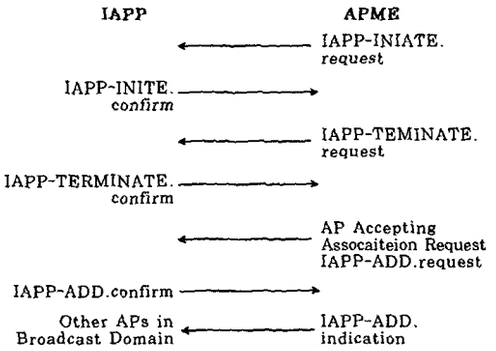

그림 4. APME와 IAPP의 관계

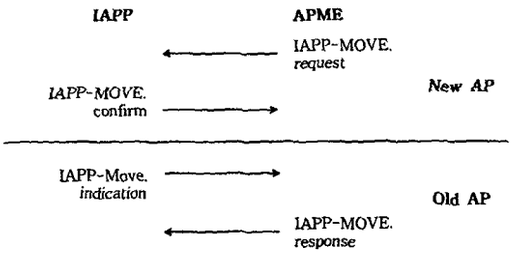

그림 5. AP 상호 운영을 위한 APME와 IAPP의 관계

II. 본 론

이 장에서는 RADIUS와 AP의 관계 및 AP 사이의 상호작용에 관하여 구체적으로 논한다.

2.1. AP의 ESS 등록

IAPP 메시지의 암호화와 인증을 지원하기 위해서는 RADIUS가 필수적으로 요구된다. AP는 RADIUS 클라이언트로 운영되며 RADIUS 서버와 비밀을 공유한다. 각 BSS는 BSSID로 구분되며, BSSID 개체는 a) BSSID, b) BSSID 비밀(최소 160 비트), c) IP 주소 또는 DNS 이름, d) IAPP 통신 보호를 위해 AP가 지원하는 cipher suite로 구성된다. IAPP 관점에서 볼 때 이 BSSID 개체들의 모임이 ESS의 멤버로 정의된다.

IAPP를 위해 AP는 ESS의 유효한 멤버로 등록해야 한다. 부가적인 이유는 ESS 내의 다른 AP들과 안전한 브로드캐스트 연결을 위해 필요한 보안 매개변수를 얻기 위함이다.

AP는 먼저 RADIUS 서버에게 RADIUS Registration Access-Request 패킷을 전송한다. 이 패킷은 BSSID와 BSSID 비밀을 포함한다. 따라서 RADIUS 서버는 이 BSSID를 ESS의 한 일원으로 등록하는 것이 가능하다. 또한 이 패킷에는 AP가 지원하는 ESP transform/인증 알고리즘 리스트도 포함 된다.

RADIUS 서버가 이 패킷을 수신하면, 서버는 AP가 ESS의 정당한 멤버인지를 검증한다. 정당하다면 RADIUS Registration Access-Accept로 응답한다.

이 때, 앞으로 사용할 ESP transform/인증 알고리즘을 선택한다. 만약 ESS의 정당한 멤버가 아니거나, 수신한 ESP transform/인증 알고리즘의 모든 리스트를 지원하지 않는다면, RADIUS 서버는 RADUIS Registration Access-Reject로 응답한다.

2.2. STA의 결합/로밍에 따른 AP들 사이의 상호작용

여기서는 STA의 결합/로밍에 따른 AP들 사이의 상호작용에 관해서만 기술한다. AP가 STA로부터 ASSOCIATION.request를 수신하면 RADIUS 서버를 통해 STA와의 SA를 생성한다. SA의 수명을 결정하기 위해 등록 세션 timeout을 사용한다. 결합에 성공하면, IAPP-ADD-notify 패킷을 IAPP 멀티캐스트 주소(224.0.1.178)로 전송한다. 이 패킷의 전송 목적은 결합한 STA의 효율적인 관리를 위해서이다. 만약 다른 AP가 이 STA와의 오래전 결합을 유지 관리하고 있다면, 새로운 결합을 알려줌으로써 해당 AP가 이 STA의 환경 정보를 삭제할 수 있도록 하는 것을 가능하게 한다. 따라서 AP들은 STA의 환경 정보를 보다 효율적으로 관리할 수 있게 된다.

IAPP-ADD-notify 패킷이 DS의 어느 곳으로부터도 전송될 수 있는 UDP/IP 프레임이라는데 주목할 필요가 있다. 이는 STA에 대한 AP의 상태 공격이 가능함을 의미한다. 따라서 IAPP-ADD-notify 패킷에 보안이 요구되며 이를 위해 ESP가 사용된다.

STA가 old AP로부터 new AP로 로밍한다고 가정하자. 재결합 요청을 위해서 STA는 new AP에게 REASSOCIATION.request를 송신한다. New AP는 이 패킷으로부터 old BSSID를 확인한다. 그런 후 old AP를 인증하기 위해서 RADIUS 서버로 RADIUS Access-Request를 송신한다. 이 패킷의 User-Name은 old BSSID가 되며, NAS-ID-Type 속성으로 new AP의 IP 주소를 송신한다.

RADIUS 서버는 old BSSID가 ESS의 정당한 멤버인지를 검증하고, IAPP를 통해 new AP와 old AP가 통신하는 것이 가능하다고 판단되면, New AP에게 Access-Accept 패킷으로 응답한다. 이 패킷에는 old AP의 BSSID, IP 주소가 포함되어 있다. 만약 new AP와 old AP가 안전한 채널을 형성해서 서버를 거치지 않는 통신을 요구하면, New-BSSID-Security-Block (NBSB)과 Old-BSSID-Security-Block(OBSB)을 송신한다. NBSB와 OBSB에는 RADIUS 서버에서 생성된 ESP의 SA를 위한 SPI와 키가 포함된다. NBSB는 new BSSID의 비밀로 암호화되어있으며, 마찬가지로 OBSB는 old BSSID로 암호화 되어 있다. 만약 old AP가 ESS의 정당한 멤버가 아니라고 판단되면 RADIUS 서버는 Access-Reject로 응답한다. 이때 RADIUS 서버가 STA를 인증하지 않는다는 것에 주의해야 한다.

New AP는 Access-Accept를 수신하면, NBSB를 복호화하고 SA를 생성한다. 만약 cache에 이를 저장한다면, lifetime을 사용하여 SA의 삭제 시기를 결정한다. 그리고 old AP에게 TCP/IP로 IAPP Send-Security-Block 패킷을 전송한다. Old AP는 이 패킷 안의 OBSB에서 다음과 같은 방법으로 키를 얻어낸다.

$$secret1 = HMAC\text{-}SHA1(null, secret)$$
$$secret2 = HMAC\text{-}SHA1(null, secret \| secret1)$$
$$secret3 = HMAC\text{-}SHA1(null, secret \| secret2)$$
$$\cdots$$
$$secretN = HMAC\text{-}SHA1(null, secret \| secretN\text{-}1)$$

$$key = secret1 \| secret2 \| secret3 \| \cdots \| secretN$$

각 비밀은 160-비트로 big-endian 형식으로 표현된다. Cipher 키는 처음 N 비트이고, 인증 키는 그 다음 M 비트이다. (N과 M의 값은 cipher suite에 의존한다) Old AP는 이전에 자신이 저장하고 있는 SA와 비교하기 위해 Send-Security-Block 안의 정보 성분 중에서 Date/time을 사용할 수 있다.

Old AP는 이런 과정을 통해서 얻은 New-AP-ACK-Authenticator를 IAPP ACK-Security-Block 패킷에 넣어 new AP에게 전송한다. New AP는 위에서와 동일한 패스워드 확장 루틴을 통해 이것을 인증하고 복호화 한 후에 얻어낸 nonce와 NBSB 안의 nonce를 비교한다. 일치하지 않다면, 공격이나 실패가 있는 것으로 가정한다. 따라서 new AP는 새로운 IAPP ACK-Security-Block를 수신할 때까지 대기하던가, 아니면 IAPP Send-Security-Block 패킷을 재 전송한다. Nonce가 일치하면 IAPP MOVE-notify를 전송한다.

Old AP가 new AP로부터 IAPP MOVE-notify 패킷을 수신하면 IAPP MOVE-response로 응답한다. 이 두 패킷의 교환 목적은 new AP와 old AP의 STA 환경 정보 교환에 있다. 예를 들어 STA의 환경 정보가 STA 보안 정보라면 재결합시 STA의 재인증을 더 빠르게 할 수 있다. New AP는 layer 2 업데이트 프레임도 전송하는데, 이는 브릿지나 스위치 같은 layer 2 장비가 MAC 주소에 의해 식별되는 STA로의 포워딩 정보를 업데이트 하기 위해서이다. Proactive Caching에 대해서는 다음 장에서 기술한다.

2.2. Proactive Caching

Proactive Caching의 목적은 로밍하는 STA에 대한 예측을 통해 Next AP에서 STA의 환경을 미리 저장함으로써 보다 빠른 로밍을 지원하는데 있다. Next AP는 선행된 구성없이 동적으로 이웃하는 AP들을 학습함으로써 식별된다. AP는 Neighbor graph를 통하여 이웃 AP들을 효율적으로 관리하며, Neighbor graph는 재결합 과정을 진행해나가면서 동적으로 학습된다. 만약 RADIUS 서버가 지원된다면 인증된 AP들만이 Neighbor graph에 추가될 수 있다.

Proactive Caching 방법에 대해서 고려해보면, 우선 AP는 재결합을 요청하는 STA의 MAC과 old AP의 MAC을 쌍으로 하여 자신의 cache에서 STA의 환경 정보를 찾는다. 만약 환경 정보가 존재한다면 STA에게 REASSOCIATE.response를 보낸 후 재결합 과정을 진행한다. 환경 정보를 찾지 못한다면, IAPP 과정에 의거하여 old AP에게 IAPP-MOVE.notify를 송신한다. IAPP-MOVE.response를 수신하면, 자신의 cache에 STA의 MAC과 old AP의 MAC, STA의 환경 정보를 저장한다. 이때 만약 STA의 MAC 자체가 존재하지 않았었다면, 가장 오래된 개체를 삭제한 후 그곳에 저장한다. STA의 MAC이 존재한다면 old AP의 MAC과 STA의 환경 정보를 업데이트 한다. 모든 과정이 끝나면 old AP를 Neighbor graph에 업데이트 하고, Neighbor graph 상의 AP들에게 IAPP-CACHE-NOTIFY.request를 송신한다.

IAPP-CACHE-NOTIFY.request를 송신한 AP는 IAPP-CACHE-NOTIFY.response 메시지로 응답하는데, 이때 수신한 cache가 더 최신이면(높은 수열번호를 갖고 있으면) 자신의 cache를 업데이트 한다. 따라서 STA의 환경이 변하는 시점에서 해당 AP는 반드시 IAPP-CACHE-NOTIFY.request를 발행해야만 한다.

III. 결 론

802.11 시스템이 점점 더 대중화 될수록, 다수의 상업용과 개인용 WLAN 시스템을 포함하는 DS가 존재하리라는 것은 명확하다. 그에 따라 AP를 통한 STA의 결합/재결합 역시 빈번해질 것이다. 따라서 DS 내에서의 AP간의 상호운영 즉, IAPP의 중요성 또한 점점 더 부각될 것이다.

802.11f의 가장 큰 장점은 ESS내의 멀티 벤더들의 AP간의 상호운영이 비교적 안전하게 운영될 수 있다는 것이다. 또한 proactive caching을 통한 빠른 로밍을 지원하는 이점도 존재한다.

이러한 AP간의 상호운영에 있어서 보안 이슈는 AP의 인증, STA 환경 정보의 안전한 전달 등이다. 본 논문에서 연구한 바와 같이 이러한 안전성을 성취하는 핵심은 ESP이다. 따라서 ESP의 적용과 그 자체의 안전성에 관한 연구가 좀 더 심도있게 진행되어야 할 것으로 보인다.

현재 진행 중인 표준화 작업 가운데서 가장 흥미로운 것은 Proactive Caching을 통해 보다 빠른 로밍을 지원한다는 것이다. Neighbor graph의 유지 문제, 보다 정밀한 학습 알고리즘과 STA의 패턴 분석 등이 요구되는 Proactive Caching은 수많은 장점에도 불구하고 실제 적용에는 큰 무리가 있을 것으로 보인다. 결합/재결합이 빈번한 핫스팟 지역에서의 각 STA의 패턴을 분석한다는 것은 쉬운 일이 아니다. 향후 이러한 점도 더 연구되어야 할 것이다.

참 고 문 헌

[1] IEEE 802.11F "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Across Distribution Systems Supporting IEEE802.11 Operation", D5.0, 2003.1

[2] IEEE 802.11-1999 "Wireless LAN Medium Acess Control(MAC) and Physical Layer(PHY) Specifications", 1999

[3] RFC 2406, "IP Encapsulating Security Payload(ESP)", November. 1998

[4] RFC 2548, "Mscrosoft Vendor-specific RADIUS Attributes", March.1993

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

[6] RFC 2869, "RADIUS Extensions", June. 2000

[7] RFC 3162, "RADIUS in IPv6", August. 2001