IAPP를 이용한 무선랜 선인증 방법

오경희[0] 강유성 이석준 정병호
한국전자통신연구원 무선LAN보안연구팀
{khoh[0], youskang, junny, cbh}@etri.or.kr

Pre-Authentication of Wireless LAN over IAPP

Kyunghee Oh[0], Yousung Kang, Sokjoon Lee, Byungho Chung
Wireless LAN Security Research Team, ETRI

요 약

무선랜에 대한 사용과 응용이 늘어나면서 등장한 요구사항들을 충족시키기 위하여 IEEE 802.11에 새로운 규격들이 계속하여 추가되고 있다. 그중 802.11i와 802.11f는 각각 무선랜 보안 강화와 액세스포인트 사이의 정보 교환을 목적으로 제정되었다. 802.11i에 의한 보안기능 강화로 인하여 스테이션의 로밍 과정에서의 지연 시간이 길어지게 되었고 이를 해결하기 위한 선인증 방식이 사용될 수 있다. 그러나 802.11i 선인증 방식에서는 스테이션이 로밍하여갈 액세스포인트를 미리 예상하고 인증을 받아야 한다는 단점이 있다. 본 논문에서는 IAPP 프로토콜을 사용하여 액세스포인트 사이에 인증 정보를 교환함으로써 스테이션이 관여하지 않고 선인증을 수행하는 방법을 제안하고, 802.11i 선인증 방식에 대한 장단점을 비교한다.

1. 서 론

IEEE 802.11 표준[1]을 따르는 무선랜은 기업의 사설망, 핫스팟과 같은 공중망, 그리고 일반 가정과 소규모 사업장에서도 사용하는 등 사용자가 계속 늘어나고 있다. 한편 그 사용 분야가 증가함에 따라 무선랜에 대한 다양한 요구사항들이 등장하게 되었다. 현재 이러한 요구사항들을 만족시키기 위하여, 새로운 표준이 제정되었거나 제정 중에 있다.

특히, 기존의 무선랜 제품이 사용하여온 WEP 방식에 의한 보안에 취약점이 있음이 알려졌고[2], 이를 해결하는 새로운 보안 표준이 IEEE 802.11i 워킹그룹에 의하여 작성되었다[3]. 또한 액세스포인트 사이의 정보를 전달하는 프레임워크가 IEEE 802.11f 워킹그룹에 의하여 작성되었다[4]. 이 외에 고속 통신, QoS, 액세스포인트 사이의 로밍 등 여러 분야에서 표준화가 진행 중이다.

무선랜의 보안기능에 관련하여 추가된 802.11i 규격의 일부 기능들은 현재 제품에 구현되어 사용 중에 있다. 그런데, 강화된 보안 기능은 액세스포인트와 스테이션 사이의 접속 과정에서 더 많은 처리과정을 필요로 하며, 이는 로밍 과정에서 데이터 통신의 지연을 가져오게 된다. 이러한 단점을 보완하기 위하여, 스테이션이 새로운 액세스포인트로 로밍하기 이전에 미리 해당 액세스포인트에 인증을 받아두는 선인증 방식이 사용될 수 있다. 그러나 이 경우 스테이션이 로밍하여 옮겨가고자 하는 액세스포인트를 미리 예측하여야만 선인증을 받을 수 있다는 단점이 있다.

액세스포인트 사이에 정보를 교환하는 IAPP 프로토콜을 사용하여 스테이션의 인증 정보를 교환한다면, 스테이션이 직접 선인증 과정에 관여하지 않고, 인증 정보가 스테이션이 로밍하여갈 액세스포인트에 전달될 수 있다. 본 논문에서 이러한 방법을 제안하고, 802.11i 선인증 방식에 대한 장단점을 비교한다.

2. 무선랜 선인증 및 IAPP 규격

2.1 IEEE 802.11i 선인증

IEEE 802.11i는 무선랜 보안을 강화하기 위하여 추가된 무선랜 규격이다. 스테이션의 사용자 인증, 스테이션과 액세스포인트 사이의 키 생성 과정 및 데이터 암복호화 과정에 대한 규격을 주된 내용으로 한다.

사용자 인증 방식 중, IEEE 802.1x[5]를 따르는 사용자 인증 방식에서는 스테이션이 액세스포인트의 중계를 통하여 원격지에 있는 인증 서버로부터 인증을 받게 된다. 그리고 스테이션이 인증에 성공하면 액세스포인트는 스테이션과 데이터 보안에 사용될 암호화키를 교환한 후, 망 접속을 허용하여 TKIP 또는 CCMP 알고리즘을 이용하여 데이터 프레임을 암호화하여 주고받게 된다.

스테이션이 선인증을 받지 않고 로밍을 하게 되면, 스테이션은 새로운 액세스포인트와 인증 및 키 교환 과정을 모두 다시 수행하여야 한다. 망 구성의 상황에 따라 인증 서버와 스테이션의 통신은 상대적으로 상당한 시간이 소요될 수 있으며, 이는 로밍 과정에서 데이터 통신이 단절되는 지연 시간을 늘리게 된다. 이를 보완하기 위하여 그림1과 같이 현재의 연결된 액세스포인트(old AP)에 접속된 상태에서 Distributed System(DS)을 통하여, 스테이션이 이동하여갈 가능성이 있는 액세스포인트(new AP)들에게서 미리 인증을 받아둘 수 있다.

이후 스테이션이 new AP로 이동하게 되면, 선인증 과정에서 생성된 공유키인 PMK의 ID 값을 reassociation 요청에 포함시켜 보낸다. new AP는 자신이 가진 스테이션의 PMK의 ID와 비교하여 그 값이 일치하는 경우, PMK를 이용하여 키 교환 과정만을 수행함으로써 스테이션의 접속을 허용한다. 이러한 과정을 통하여, 로밍 과정에서 스테이션과 인증 서버를 사이의 인증과정을 생략할 수 있다.

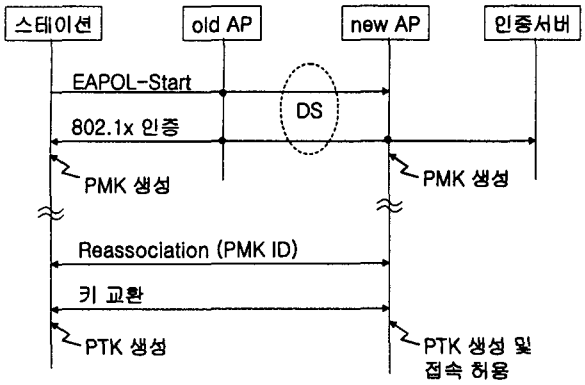

그림 1 IEEE 802.11i 선인증 과정

2.2 IEEE 802.11f IAPP

IEEE 802.11f는 DS를 통하여 액세스포인트 사이에 정보를 주고받는 프로토콜인 IAPP를 정의한다. IAPP는 인터넷 프로토콜의 TCP/UDP를 사용한다.

IAPP에는 스테이션이 액세스포인트에 association이 이루어졌을 때 액세스포인트가 주위의 다른 액세스포인트들에게 이를 알리는 Add-notify 패킷, 스테이션의 로밍으로 reassociation이 이루어졌을 때 액세스포인트 사이에 주고받는 Move-notify/response 패킷, 로밍에 대비하여 스테이션 정보를 액세스포인트 간에 미리 전달하는 Cache-notify/response 패킷이 정의되어 있다.

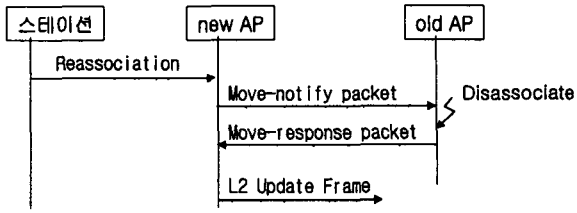

그림 2 IEEE 802.11f IAPP 로밍 과정

그림2는 스테이션이 로밍하여 new AP에 reassociation이 이루어졌을 때의 액세스포인트 사이에 주고받는 IAPP 메시지를 보여준다. new AP로부터 Move-notify 패킷을 통하여 스테이션의 로밍을 통보 받으면, old AP는 Move-response 패킷을 new AP에 반환한다. 이때 패킷 내의 context block 영역에 추가 정보를 포함시켜 전달할 수 있다. 그리고, old AP는 해당 스테이션을 disassociate 하고, association 테이블에서 제거한다. 또한 new AP는 Move-response 패킷을 수신한 후, 2계층 경로 갱신 프레임을 브로드캐스트하여 DS의 스위칭 경로를 갱신한다.

필요에 따라, 액세스포인트는 reassociation 과정과 무관하게 Cache-notify 패킷을 통하여 context block을 이웃한 액세스포인트들에게 전달할 수 있다. 이는 스테이션이 로밍을 수행하기 이전에 미리 스테이션의 정보를 전달하는데 사용될 수 있다.

3. IAPP를 이용한 선인증 방법

3.1 제안된 방법

802.11f 규격은 액세스포인트 사이에 정보를 전달하는 프로토콜을 정의하고 있지만, 그 프로토콜 내에 들어가는 context에 대해서는 아무것도 정의하고 있지 않다. 어떠한 context를 전달할 것인가는 새로운 표준에서 정의하거나, 실제 액세스포인트를 구현할 때 응용하여 사용할 수 있다.

이를 토대로 한 IAPP를 사용하는 응용으로, IAPP의 context block에 스테이션의 인증정보를 담아 전달한다면, 802.11i의 선인증 방식과 비슷한 효과를 얻을 수 있다.

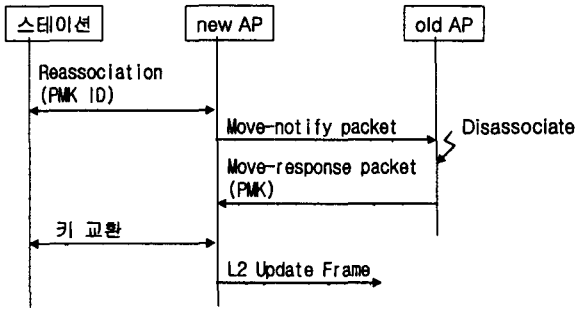

그림 3 Move-reponse를 통한 PMK 전달

그림3은 Move-response의 context block에 PMK를 포함시켜 전송하는 과정을 보여준다. 스테이션이 old AP와의 접속과정에서 생성된 PMK의 ID를 사용하여 new AP에 reassociation을 요청한다. 그러면, new AP는 old AP로 Move-notify 패킷을 전송하며, old AP는 Move-response 패킷의 context block에 해당 스테이션의 PMK 포함시켜 전송한다. new AP는 PMK ID를 확인하고 그 값이 일치하면, 인증과정 없이 PMK를 사용하여 키 교환 과정을 수행한다.

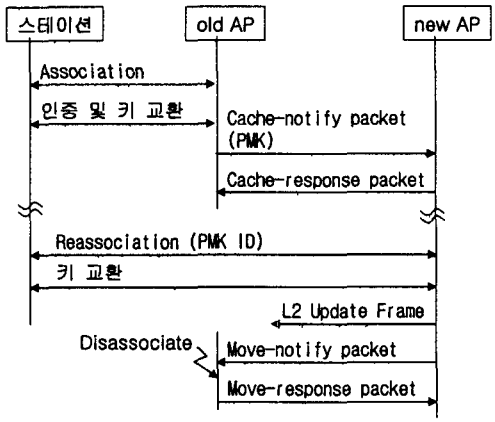

그림 4 Cache-notify를 통한 PMK 전달

그림4는 Cache-notify를 사용하여 이웃한 액세스포인트

들에게 스테이션의 PMK를 미리 전달과정을 보여준다. 이러한 방법에서는. 스테이션이 로밍한 후 new AP와 old AP가 Move-notify/response 패킷을 교환하는 과정이 필요 없이 바로 키 교환 과정을 수행할 수 있으므로, 로밍 시간을 더욱 단축시킬 수 있다.

한편, 이웃한 액세스포인트에 대한 정보는 관리자의 설정에 의해서 지정될 수도 있지만, 여러 스테이션의 로밍 과정을 통한 러닝을 통하여 이웃한 액세스포인트를 인지할 수도 있다.

3.2 802.11i 선인증에 대한 장단점

이 방법이 802.11i 선인증 방식과 다른 점은 스테이션이 선인증 과정에 직접 개입되지 않고, 액세스포인트 사이에서만 인증정보가 교환된다는 점이다. 802.11i에서처럼 스테이션이 선인증에 개입될 경우, 스테이션은 자신이 로밍하여 갈 것으로 예상되는 액세스포인트를 예측할 수 있어야 한다.

스테이션이 로밍 가능성이 있는 액세스포인트를 찾는 방법은 수신되는 beacon 프레임을 주기적인 스캐닝하는 것으로 어느 정도 가능하다. 그러나 스캐닝 중에 데이터 통신이 일시적으로 방해받을 수도 있으며, 또한 스테이션이 두 액세스포인트에서 겹치는 셀 영역을 신속히 통과하는 경우, old AP를 통하여 new AP의 선인증 받는데 필요한 충분한 시간을 확보하지 못할 수도 있다.

IAPP를 사용하는 제안된 방법의 경우, 스테이션이 직접 주변의 액세스포인트를 감지할 필요가 없다. AP는 정적으로 설정되거나, 러닝에 의하여 동적으로 파악된 이웃한 액세스포인트들에게 스테이션의 PMK를 미리 알려줌으로써 스테이션은 이웃한 액세스포인트로 로밍한 후, old AP에서 사용하던 PMK를 계속하여 사용하게 된다. 일반적으로 액세스포인트는 한 위치에 고정되어 있으므로, 액세스포인트 사이의 로밍 정보 교환을 통한 선인증은 성공률이 매우 높다.

그러나 한편, old AP와 new AP가 동일한 PMK를 사용하게 됨에 따라, 어느 한 액세스포인트에서 PMK가 유출된다면, 스테이션이 로밍한 후에도 해당 스테이션의 데이터가 계속하여 노출되므로, 이는 보안의 취약점이 될 수 있다.

4. 결론

무선랜의 사용 범위가 넓어지면서 다양한 응용들로부터의 요구 사항을 만족시키기 위하여, 안전하고 신속한 보안 로밍은 더욱 중요하여지고 있다. 특히 VoIP 서비스의 경우 끊어짐이 없는 로밍의 필요성이 더욱 크다. 이러한 문제를 해결하기 위하여, 현재 IEEE 802.11r 태스크 그룹에서 표준화 활동이 진행되고 있다.

IAPP를 사용하면 보안 관련 정보와 QoS 등의 정보들을 이웃한 액세스포인트로 전달할 수 있다. 이러한 정보가 액세스포인트 사이에 전달되지 못한다면, 스테이션이 로밍할 때마다 액세스포인트와의 접속에 관한 재협상을 거쳐야만 한다. 그러나 본 논문을 통하여 스테이션에 관련된 보안 정보를 미리 이웃한 액세스포인트에 전달함으로 얻는 이점을 살펴보았다.

IAPP를 이용하여 PMK를 전달하는 방식은 스테이션이 직접 재접속할 액세스포인트를 검색할 필요가 없으며, 액세스포인트는 스테이션의 재접속 정보를 이용하여 이웃 액세스포인트를 파악할 수 있으며, 이는 선인증이 실패할 가능성을 줄어들게 한다는 점에서 현재의 표준 규격인 802.11 선인증 방식에 대하여 장점이 있다.

참고 문헌

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Std 802.11-1997, June 1997.

[2] W. A. Arbaugh, et al. "802.11 Security Vulnerabilities," http://www.cs.umd.edu/~waa/wireless.html.

[3] "Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications: Amendment i: Medium Access Control (MAC) Security Enhancements," IEEE Draft 802.11i/D8.0, February 2004.

[4] "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Std 802.11F, 2003.

[5] "Port-Based Network Access Control," IEEE Std 802.1x - 2001, June 2001.