제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

AP 사이의 데이터 중계를 통한 신속하고 안전한 무선랜 로밍 방법

오경희, 강유성, 정병호
한국전자통신연구원 무선 LAN 보안연구팀
e-mail : khoh@etri.re.kr

Fast and Safe Roaming in Wireless LAN By Forwarding Data Frames between APs

Kyunghee Oh, Yousung Kang, Byungho Chung
Wireless LAN Security Research Team, ETRI

요 약

기존의 IEEE 802.11 표준에 따르는 무선랜에서 보안에 취약한 점들이 발견된 후, 이를 보완하기 위한 802.11i 규격이 작성되고 있다. 이에 따르면, STA 가 로밍하는 과정에서 new AP 와 reassociation 이후 AP 로부터 인증을 받는 과정을 추가로 거쳐야 한다. 이는 로밍 과정에서 발생하는 지연을 늘리고, 따라서 데이터 프레임들의 손실을 가져온다. 그런데, new AP 와 STA 사이의 보안협상이 완료될 때까지, old AP 에서 손실될 데이터 프레임을 old AP 의 보안 정보를 적용하여 new AP 를 통해서 STA 로 전달함으로써 이러한 데이터 손실을 막을 수 있다.

1. 서론

IEEE 802.11 표준[1]을 따르는 무선랜은 기업의 사설망, 핫스팟과 같은 공중망, 그리고 일반 가정과 소규모 사업장에서도 사용하는 등 사용자가 계속 늘어나고 있다. 그런데, 기존의 무선랜 제품이 사용하여온 WEP 방식에 의한 보안에 취약점이 있음이 알려졌고 [2], 이를 해결하는 새로운 보안 표준이 IEEE 802.11 워킹그룹에 의하여 작성되고 있다.

IEEE 802.11i 의 드래프트 문서[3]에 따르면, 보안 기능을 강화하기 위하여 무선랜에서의 사용자 인증과 데이터 보호 기능을 추가하였다. 사용자 인증을 위하여 IEEE 802.1x 규격에 따라 인증 서버를 통하여 사용자를 검증하는 방법과 pre-shared key 를 사용하여 사용자를 검증하는 방법이 사용된다. 그리고, 데이터 보호를 위하여 기존의 WEP 을 변형한 TKIP 알고리즘 또는 AES 를 적용한 CCMP 알고리즘을 사용한다.

이러한 기능을 지원하기 위하여, 단말 STA 와 AP 가 보안 협상을 하는 과정에 사용자 인증 및 키 교환 과정이 추가되었다. 이는 STA 가 ESS 내에서 로밍하는 과정에서 지연을 일으키는 요인이 되어, 로밍 과정에서 데이터 전송이 차단되는 기간이 길어진다.

본 논문에서는 IEEE 802.11i 를 적용하는 무선랜 환경에서 STA 가 이전의 old AP 영역에서 새로운 new AP 영역으로 이동하는 보안 로밍 과정 중에 발생하는 지연으로 인하여 발생하는 데이터 프레임 손실을 줄이는 방법을 제안한다.

2. 무선랜 보안 규격

2.1 IEEE 802.11i

IEEE 802.11i 는 무선랜 보안을 위하여 인증 및 키교환 과정과 데이터 암복호화 과정에 대한 규격을 주 내용으로 하고 있다.

사용자 인증 방법은 IEEE 802.1x[4]를 따르는 방식과 pre-shared key 방식이 있다.

IEEE 802.1x 에는 역할에 따라 세 가지 시스템이 있다. 서비스를 제공하고자 하는 포트에 대하여 인증을 수행하는 authenticator, authenticator 에서 제공하는 포트의 인증을 받고자 하는 supplicant, supplicant 의 신분을 인증하여 authenticator 가 서비스를 제공할 수 있도록 알려주는 authentication server(AS)로 구성된다. authenticator 는 supplicant 와 주고받는 EAPOL 프레임

으로 supplicant 와 AS 사이의 EAP 메시지를 중계하여 인증과정을 수행한다. 그리고 인증에 성공한 supplicant 들에 대해서만 망으로의 데이터 프레임 전송을 허용한다. 무선랜 환경에서는 AP 가 authenticator 의 역할을 수행하며, 인증이 완료된 후 AP 와 STA 사이에 공유키가 생성된다.

기업망이나 공중망과는 달리, 소호 및 홈네트워크에서는 굳이 별도의 인증 서버를 둘 필요가 없다. 이러한 환경에서는 AP 와 STA 에 미리 공유키를 설정해 두는 pre-shared key 방식을 사용할 수 있다.

AP 와 STA 는 공유키를 사용해 실제 데이터 프레임의 암호화에 사용되는 임시키를 생성하기 위한 키교환 과정을 수행하며, 각각의 STA 이 할당되는 pairwise 키와 여러 STA 이 공유하는 group 키를 생성한다.

pairwise 및 group 키가 설정된 후, STA 와 AP 는 TKIP 또는 CCMP 알고리즘을 이용하여 데이터 프레임을 암호화하여 주고 받게 된다.

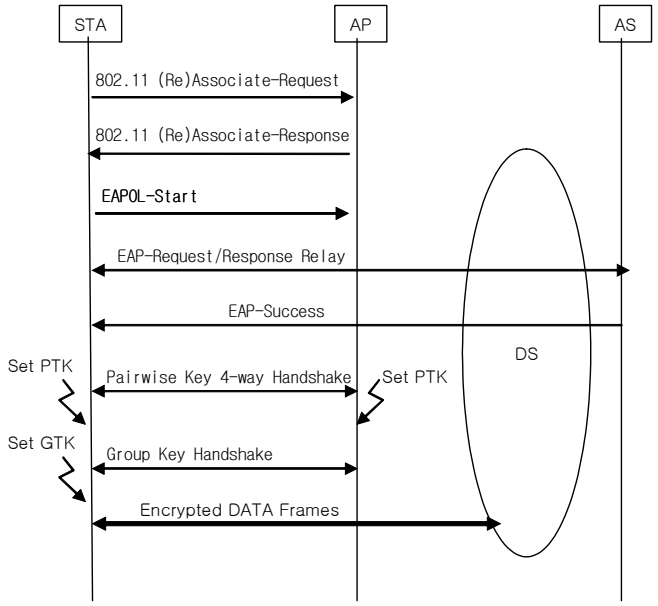

그림 1 IEEE 802.11i 보안 협상 과정

그림 1 은 802.1x 에 의한 인증과 키 교환을 통한 STA 와 AP 의 접속 과정을 보여준다. 802.1x 에 따른 인증은 Distribution System(DS)을 통하여 연결된 AS 로부터 STA 가 인증을 받게 된다. 망 구성의 상황에 따라 AS 와 STA 의 통신은 상당한 시간이 소요될 수 있으며, 이는 접속과정 전체에 소요되는 지연 시간을 늘이게 된다.

2.2 IEEE 802.11f IAPP

IEEE 802.11f 에서 802.11 DS 를 통하여 AP 간에 정보를 주고 받는 프로토콜인 IAPP 를 정의하며, 인터넷 프로토콜의 TCP/UDP 를 사용한다.

IAPP 에는 STA 가 AP 에 association 이 이루어졌을 때 AP 가 주위의 다른 AP 들에게 이를 알리는 Add-notify 패킷, STA 의 로밍으로 reassociation 이 이루어졌을 때 AP 사이에 주고 받는 Move-notify/response 패킷, 로밍에 대비하여 STA 정보를 AP 간에 미리 전달하는 Cache-notify/response 패킷이 정의되어 있다. 이 패킷들의 context block 영역에 추가 정보를 포함시켜 AP 사이에 전달할 수 있다.

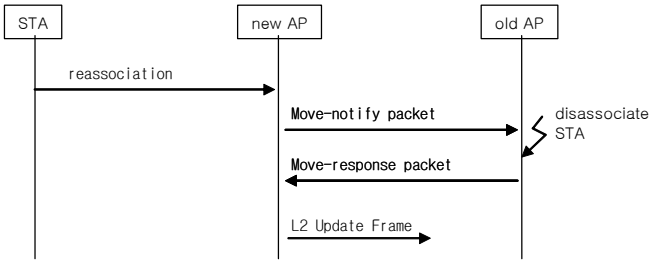

그림 2 IEEE 802.11f IAPP 로밍 과정

그림 2 는 STA 가 로밍하여 new AP 에 reassociation 이 이루어졌을 때의 AP 간에 주고 받는 IAPP 패킷을 보여준다. new AP 로부터 Move-notify 패킷을 통하여 STA 의 로밍을 통보 받으면, old AP 는 STA 를 disassociate 하고 자신의 association 테이블에서 STA 를 제거하게 된다. 또한 new AP 는 Layer 2 Update Frame 을 DS 로 broadcast 하여 DS 의 스위칭 경로를 갱신한다.

3. 제안된 데이터 중계 방법

그림 3 은 STA 가 old AP 영역에서 new AP 영역으로 로밍하는 모습을 보여준다. 이러한 로밍 과정에서 STA 는 new AP 와 접속하는 과정에서 일시적으로 데이터를 송수신하지 못하게 된다. 특히 802.11i 에 따른 접속 과정에서는 무선랜에서의 보안을 강화하기 위한 과정이 추가되어, STA 를 인증하고 키를 교환하는 보안 협상 과정으로 인하여 지연시간은 더욱 길어진다. 따라서 그만큼 데이터 통신이 중단되는 시간이 길어지게 된다.

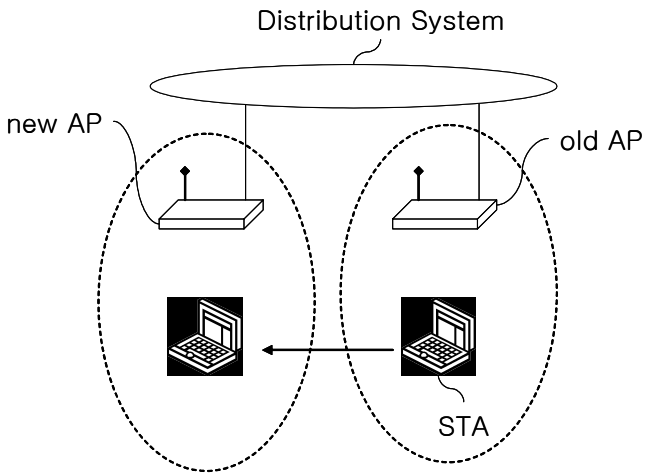

그림 3 무선랜 로밍

그런데, STA 가 new AP 의 영역으로 이동한 후, 인증 및 키교환 과정에서 old AP 에서 new AP 로 데이터 프레임을 중계한다면 로밍 과정에서 손실되는 데이터 프레임의 양을 줄일 수 있다.

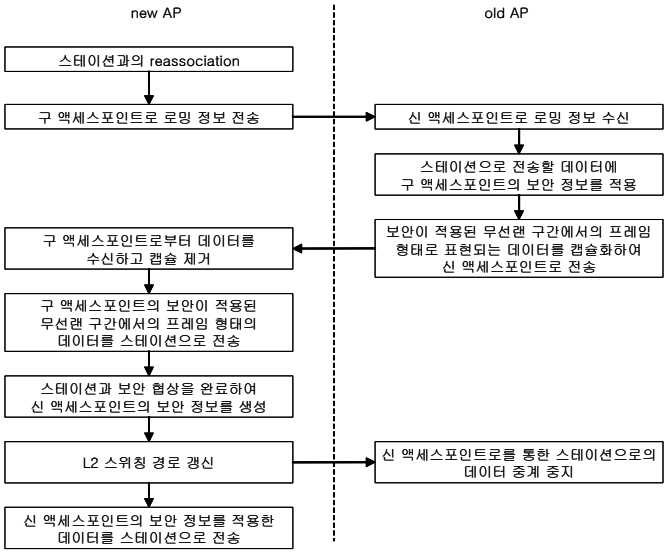

그림 4 제안된 로밍 과정에서의 데이터 중계 방법

그림 4 는 로밍 과정에서 old AP 에서 new AP 로 데이터를 중계하는 과정에 따른 AP 의 역할을 보여준다.

IEEE 802.11i 규격에 따른 환경에서는 STA 가 new AP 영역으로 이동하는 로밍 과정에서 reassociation 이 이루어진 후, AP 사이에 정보를 교환하는 과정 없이 new AP 와 STA 사이에 보안 협상이 이루어진다. 이 과정 중에 old AP 를 통하여 STA 로 전달되어야 할 데이터 프레임들은 손실된다.

이 과정에서의 손실을 줄이기 위하여, new AP 는 STA 의 reassociation 이 이루어진 후, 보안 협상을 수행하기 이전에 old AP 로 STA 가 이동하여 왔음을 통지한다. 이를 수신한 old AP 는 STA 로 전송할 데이터 프레임을 무선 구간으로 전송하지 않고, old AP 와 STA 사이의 보안 정보를 적용하여 암호화된 데이터 프레임을 캡슐화하여 new AP 로 전송한다. new AP 는 전송받은 데이터 프레임을 복호화하지 않고 암호화된 채, 캡슐만을 풀어 무선구간을 통하여 STA 로 전송한다. STA 는 old AP 에서 협상된 보안 정보를 이용하여 데이터 프레임을 복호화하여 수신하게 된다. 이 과정에서 전송되는 데이터 프레임의 형태를 그림 5 와 같이 생각해 볼 수 있다.

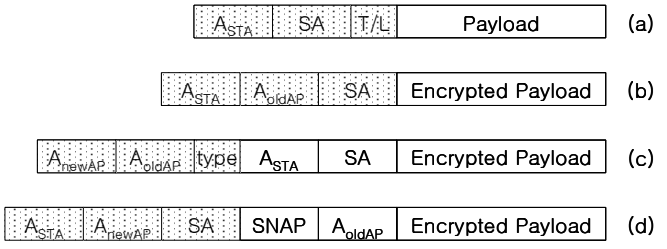

그림 5 제안된 방법에서 사용되는 데이터 프레임 형태

그림 5 의 (a)는 STA 의 주소 A_{STA} 를 목적지로 하는 DS 에서의 데이터 프레임 형태이다. (b)는 이 프레임이 old AP 에 의하여 무선구간으로 전송될 때의 데이터 프레임 형태이다. (c)는 무선구간으로 전송되지 않고, 제안된 방법에 따라 캡슐화하여 유선구간을 통하여 new AP 로 전송되는 데이터 프레임 형태이다. (d)는 이를 수신 받은 new AP 에서 STA 로 전송하는 무선구간에서의 데이터 프레임 형태이다. 각 프레임에서 회색으로 채워진 영역이 MAC 헤더에 해당된다. 제안된 방법에 의하면, (a) 형태의 프레임을 DS 로부터 old AP 가 수신하고, old AP 는 이를 (c) 형태의 프레임으로 변환시켜, DS 를 통하여 new AP 로 전달한다. new AP 는 이를 다시 (d) 형태의 프레임으로 변환시켜 STA 로 전송한다.

old AP 에서 new AP 를 통하여 STA 로 전달되는 데이터 프레임 (c)와 (d)의 경우, type 영역 또는 SNAP 헤더를 통하여 별도의 payload 형을 지정하여 AP 와 STA 에서 이를 인식하여 처리할 수 있어야 한다. new AP 는 (c)의 MAC 헤더 및 payload 에 포함된 A_{STA} 와 소스 호스트 주소 SA, old AP 의 주소 A_{oldAP} 를 사용하여 무선구간에 전송될 (d) 프레임을 생성한다. 프레임을 (c)에서 (d)로 변환하는 과정에서 암복호화가 일어나지 않으므로 new AP 는 old AP 와 STA 사이의 보안 정보를 알 필요가 없으며, 단지 프레임 형태만 변형하여 STA 에 전송하게 된다. STA 는 old AP 와의 보안 정보를 알 수 있으므로, 암호화된 payload 를 복호화하여 수신할 수 있다.

이러한 방법을 통하여 로밍 과정 중, new AP 에서 보안 정보를 미리 알 필요 없이, old AP 에서 발생하는 데이터 손실을 방지하고 STA 로 전송될 수 있도록 한다.

new AP 와 old AP 사이의 STA 로밍 정보를 주고 받는 방법으로 IEEE 802.11f IAPP 를 사용할 수 있다. IAPP 에서 context block 을 사용할 필요 없이, Move-notify 및 Move-response 패킷을 주고 받는 것만으로도 로밍 정보를 전달하기에 충분하다. IAPP 에 의하면 old AP 에서 보낸 Move-response 패킷을 new AP 에서 수신하면, Layer 2 Update Frame 을 new AP 에서 broadcast 하게 되어있다. new AP 에서 STA 와 보안 정보 협상을 끝낸 후에 Layer 2 Update Frame 을 전송함으로써, old AP 는 STA 의 로밍 과정이 완료되었음을 통보 받는다. 따라서, 더 이상 데이터 프레임을 중계하지 않고, STA 의 보안 정보도 유지할 필요가 없게 된다.

STA 가 old AP 영역에서 new AP 영역으로 이동하여 reassociation 이 이루어지는 시간을 T_{MOV}, AP 사이에 IAPP Move-request/response 패킷을 주고 받는데 걸리는 시간을 T_{IAPP}, STA 가 new AP 를 통하여 보안 협상을 하는 시간을 T_{NEG}, DS 에서 2 계층 전송 경로 갱신이 이루어지는 시간을 T_{UP} 이라 한다면, 보안이 적용되지 않는 무선랜 환경에서의 로밍에 의한 지연시간 D_O, 기존의 802.11i 환경에서의 로밍 지연시간 D_I, 제안된 방법에 의한 로밍 지연시간 D_S 는 각각 다음 수식과 같이 나타낼 수 있다.

$$D_O = T_{MOV} + T_{UP}$$
$$D_I = T_{MOV} + T_{NEG} + T_{UP}$$
$$D_S = T_{MOV} + T_{IAPP}$$

802.11i 보안을 적용함으로써 T_{NEG} 의 추가 지연 시

간이 발생한다. 그러나 제안된 방법에 의하면, T_{NEG} 에 의한 지연 대신 T_{IAPP} 에 의한 추가 지연이 발생하며, 또한 2 계층 전송 경로 갱신이 이루어지기 전에 old AP 를 통하여 데이터 프레임이 중계되므로 T_{UP} 에 의한 지연이 사라진다.

T_{NEG} 는 인증 및 키교환에 필요한 시간이며, 특히 802.1x 인증을 위해서는 원격지에 있는 AS 와 여러 번 프레임을 주고 받아야만 하며, 이는 상대적으로 많은 시간을 소요한다. 그러나, T_{IAPP} 를는 일반적으로 동일한 서버넷 내에 위치한 AP 사이에 한번의 패킷을 주고 받는 시간이 소요된다. 따라서 D_S 는 D_I 에 비하여 $(T_{NEG} + T_{UP} - T_{IAPP})$ 만큼의 지연시간 단축을 가져온다.

4. 결론

제안된 방법에 따르면 802.11i 보안을 적용하면서 발생하는 보안 협상 과정으로 발생하는 지연시간을 줄일 수 있음을 확인할 수 있다. 그러나, 이는 STA 에서 데이터 프레임을 수신하기 시작하는데 걸리는 지연이 줄어드는 것을 의미한다. STA 에서 DS 로 전송할 데이터 프레임은 new AP 와 보안협상이 완전히 이루어진 후에야 가능하다. 즉 STA 에서 데이터 프레임을 송신하기 시작하는 데 걸리는 지연시간에서는 제안된 방법으로 전송 지연을 해결할 수는 없다.

STA 에서 송신을 시작하기까지 지연되는 시간에서는 데이터 프레임들을 STA 에서 일단 버퍼링하여 보관하고, new AP 와 보안협상이 이루어진 후에 전송함으로써, 데이터 프레임이 손실될 가능성을 줄일 수 있다.

한편, STA 에서 수신할 데이터 프레임들의 경우, 제안된 방법을 사용하지 않으면, 로밍 과정이 진행 중인 시간 동안 데이터 프레임들은 old AP 에서 모두 손실되고 만다. 그러나, 제안된 방법을 사용하면, old AP 에서 new AP 를 통하여 STA 로 데이터 프레임을 전송할 수 있어 데이터 프레임의 손실을 줄일 수 있다.

일반적으로 2 계층에서 데이터 프레임 손실이 어느 정도 허용되고 있으나, 상위 계층에서의 응용 특성에 따라 데이터의 재전송에 의한 지연이나 복구가 불가능한 데이터 손실을 일으킬 수도 있다. 따라서 old AP 에서 발생할 데이터 프레임 손실을 줄이는 것은 상위 계층 응용의 환경에 도움이 된다고 볼 수 있다.

802.11i 에서 보안 협상에 의한 로밍 과정에서의 접속 지연을 줄이기 위하여 사전 인증 방식을 정의하고 있다. 이 방법은 STA 가 old AP 영역 내에 있을 때 미리 new AP 에 대한 인증을 완료하여 두는 것이다. 이후 STA 가 new AP 로 이동하였을 때, 인증 과정을 거치지 않고 바로 키교환을 수행하여 로밍 과정에서의 지연 시간을 줄인다. 이러한 방법은 STA 가 어느 AP 를 사전 인증할 것인지 로밍 과정이 이루어지기 이전에 미리 알고 있어야 한다는 조건이 있다. 제안된 방법은 이러한 조건이 필요하지 않으므로, 사전 인증 방식을 사용할 수 없는 환경에서도 지연 시간을 줄이는 데 도움이 된다.

참고문헌

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

[5] "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