무선LAN 환경에서 단말 이동시 AP간 메시지 보안 개선 방안

송일규°, 홍충선, 이대영
경희대학교 전자정보학부
niceguy74°@empas.com, {cshong, dylee}@khu.ac.kr

Improvement of Message Security between APs during STA Movement in Wireless Environment

Il-Gyu Song° Choong Seon Hong Dae Young Lee
School of Electronics & Information, Kyung Hee University

요 약

현재, IEEE 802.11 WG(Working Group)중에는 AP(Access Point)간의 표준화된 프로토콜을 개발하는 TGf(Task Group F)가 있다. 이 그룹에서는 서로 다른 제조업체에서 생산한 AP 간의 상호연동을 보장하기 위한 IAPP(Inter Access Point Protocol)를 제안하였는데, 이는 동일 서브네트워크 내의 서로 다른 AP간에 이동성을 보장하기 위한 프로토콜로, STA(Station)들이 이동할 때 재인증 과정을 거치지 않고 AP간의 Security Context 정보나 Layer 2 forwarding 정보를 공유함으로서 STA간의 seamless connectivity를 제공한다. 본 논문에서는 위의 AP간의 메시지 전달시 발생할 수 있는 키 유출을 막기 위해서 메시지의 전달 경로를 바꾸고, 좀 더 높은 보안성을 제공하기 위해 공개키를 이용한 방안을 제시하고자 한다.

1. 서 론

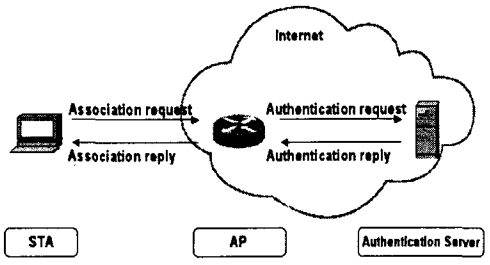
802.11 무선랜은[1] 인터넷 사용자의 증가와 무선통신기술의 발전으로 시작된 기술이다. IEEE에서는 802.11b 표준을 완료하였고[2], 현재 무선랜 시장은 빠른 성장을 보이고 있다.

무선랜 시스템을 구현하는 방법은 다양하므로 개념의 구현에 대해서는 규정되어 있지 않다. 이는 각각의 vender별 AP 설계에 유연성과 다양성을 주었지만 이로 인해 AP간의 상호연동이 어렵게 되었다. 이러한 문제를 해결하기 위해 TGf 에서는 vender들 간의 상호 연동을 위해서 IAPP(Inter Access Point Protocol)라는 프로토콜을 제안[4]하게 되었다. 이 IAPP는 서로 다른 AP간에 이동성을 보장하는 프로토콜로, AP간에 정보를 공유함으로써 단말이 신속한 이동을 할 수 있도록 지원하는 프로토콜이다. 하지만 무선매체의 특성인 공개성에 따른 해킹이 문제가 되고 있는데, 이에 대한 보안체계의 확립이 필수적이다. IAPP에서는 AP간의 Security정보의 보안을 위해서 ESP(IP Encapsulating Security Payload)[5]를 이용하고 있으며, 근래에 들어서 키 유출에 관한 문제점들이 많이 발생하고 있다.

본 논문에서는 단말의 신속한 이동을 지원하기 위한 AP간 정보의 공유시 발생할 수 있는 정보유출을 막기 위해 공유정보의 이동경로를 바꾸고 공개키를 이용한 메시지 보안방법을 제안하였다. 본 논문의 구성은 다음과 같다. 제 2장에서는 관련연구로서 802.11b의 기본적인 인증방법을 소개하고, 제 3장에서는 기존의 IAPP 프로토콜의 구조와 동작에 대해 알아보며, 제 4장에서는 AP간의 공유정보의 전달에 있어서의 메시지 보안에 관한 방법을 제안하고, 마지막으로 제 5장에서는 결론을 맺는다.

2. 관련연구

IEEE 802.11b 표준의 무선랜 보안 기술을 보면 다음과 같다. 이동 무선랜을 이용하여 네트워크에 접속하려는 STA은 새로이 근접한 AP(Access Point)에게 접속요청을 보내면 AP는 RADIUS(Remote Authentication Dial In User Service)[3]라는 인증서버를 이용하여 STA에게 접속을 허가하게 된다. 접속과정은 [그림 1]과 같다.

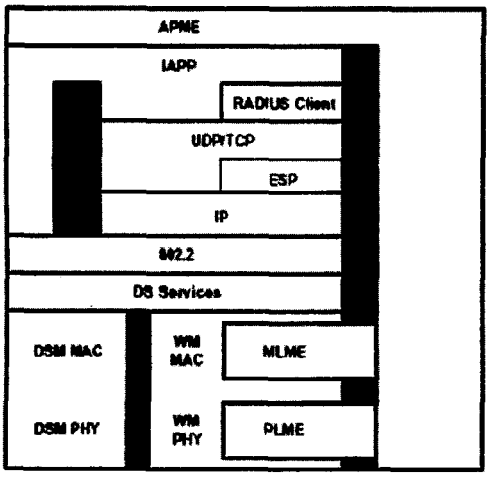


[그림 1] STA 사용자의 네트워크 접속과정

현재 사용되고 있는 802.11b표준은 무선랜의 인증과정과 비밀성을 제공하기위해 SSID(Service Set IDentifiers)와 WEP(Wired Equivalent Privacy)을 정의하고 있다. SSID는 접근제어의 기본 수준을 제공한다. 이는 유선랜 장치들에 대한 네트워크이름이며, 네트워크를 세그먼트로 분리하여 사용할 때 활용된다. WEP는 무선랜의 데이터 스트림을 보호하는 메커니즘을 제공하며 대칭 암호화 알고리즘을 사용한다. 따라서 암호화와 복호화를 처리할 때 동일한 키(Key)와 알고리즘을 사용한다. 이때 올바른 WEP키를 가지고 있지 않거나 인증에 실패하면 사용자의 접속요청은 거부된다.

3. IAPP 프로토콜 구조와 동작과정

3.1 IAPP 프로토콜의 구조



[그림 2] IAPP 구조도

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

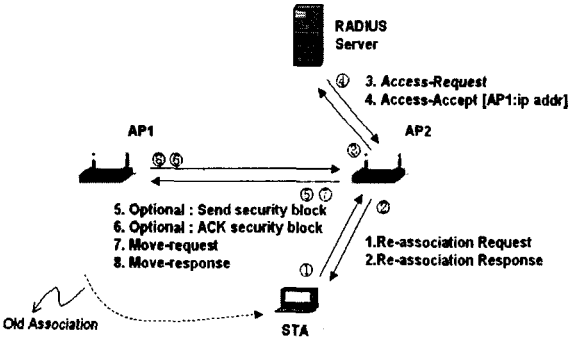
IAPP는 AP의 특성과 기능을 구현하고 있는 AP 운영 entity인 APME(AP Management Entity)와 IAPP SAP(Service Access Point)를 통해 IAPP-INITIATE 서비스 primitive를 교환하며 초기화된다. IAPP는 APME를 통해 STA re-association 요청을 수신한 경우 802.1X 인증을[6] 지원하기 위해 RADIUS client를 사용한다. client는 RADIUS server와 통신을 함으로써 AP의 BSSID와 IP주소를 mapping하는 기능과 AP들 사이의 암호화를 위한 키 분배 기능을 한다.

3.2 ESP 동작 개요

ESP는 기밀성, 원본 데이터의 인증, 무결성과 같은 보안 서비스를 지원하기 위하여 설계된 프로토콜로 IP 데이터그램 안에 삽입된다. IP 데이터 그램 안에 ESP가 삽입 될 경우 ESP 뒤의 데이터는 암호화 된다. 그리고 수신측 에서는 IKE로 미리 교환한 Key 값을 이용하여 데이터를 복호화 하는 기능을 수행하게 된다. ESP 모드에는 크게 Transport mode와 Tunnel mode 가 있다. 먼서 ESP Transport의 경우 ESP 헤더가 IP헤더 뒤에 오는 경우로서 TCP 헤더와 그 뒷 단의 데어터에 대한 Security를 보장해 준다. 하지만 이는 IP 헤더가 암호화가 되지 않기 때문에Header 정보에 대한 보안을 할 수 없다. Tunnel mode 의 경우 IP 헤더까지 암호화가 되는데 이는 New IP Header 라는 새로운 IP 헤더를 붙임으로써 원본 IP 헤더부터 데이터 까지 암호화 되어 전송함으로 Transport mode에 비해 좀 더 안전하다.

3.3 IAPP 동작 개요

동일 서브네트워크에서 서로 다른 AP간에 이동성을 보장하기 위한 프로토콜인 IAPP는 AP간 Layer 2 Forwarding 정보와 Security Context 정보를 공유함으로써 단말의 빠른 이동성을 제공한다. 이때 두 AP 사이의 WEP키 전달시 사용할 보안 알고리즘으로 ESP를 사용하는데,ESP authenticator는 인증서버인 RADIUS로부터 얻게 된다. IAPP를 지원하는 동일 서브네트워크에서의 AP와 단말간에 메시지 동작흐름은 [그림 3]과 같다. STA이 AP2 영역에 들어가게 되면, AP2에게 Re-association을 요청하고, AP2는 인증서버에게 Access Request 메시지를 보내며 Access Accept 메시지를 받음으로써 AP1과 AP2를 인가하게 되며 Security 관련정보를 획득하게 된다. 이 정보에는 AP1과 AP2 사이에 주고받는 Move-Request 와 Move-Response 메시지를 인증 및 암호화하기 위한 알고리즘인 ESP authenticator 등이 포함된다.



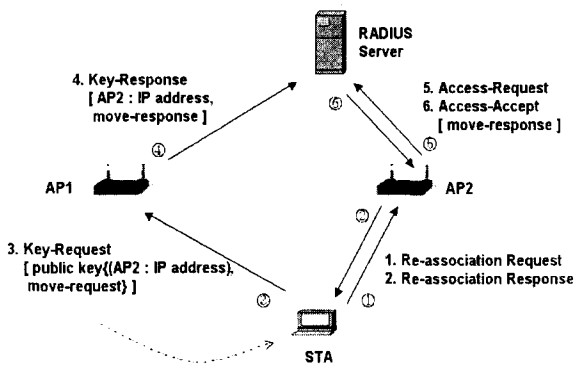
[그림 3] IAPP 동작 과정

여기서, AP1과 AP2 사이에 전달되는 메시지와, STA과 AP간 Privacy를 위해 사용되는 WEP 키와 비밀번호 등이 악의적인 공격용 소스 등에 의해 노출될 위험성이 크

다. 또한 IAPP가 지원되지 않는 AP일 경우 IAPP가 지원되는 AP와의 연결성이 떨어지는 문제점이 생길 수 있다.

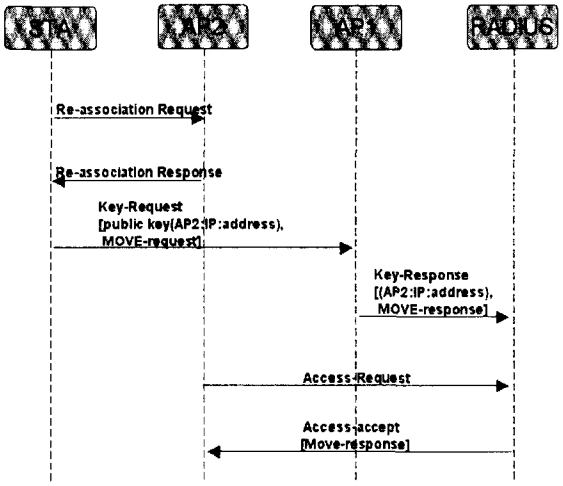
4. 제안 및 해결방안

본 논문에서는 Old AP(AP1)와 New AP(AP2) 사이에 주고받는 Security정보의 유출 가능성을 줄이고, IAPP가 지원되는 AP와 지원되지 않는 AP 간의 좋지 못한 연결성문제를 해결하기 위해 AP1과 AP2 사이의 메시지 전송 경로를 AP1과 인증서버사이의 이미 인증되어 사용되었던 경로를 이용하고, 또한 ESP알고리즘 대신 공개키를 이용하여 좀 더 높은 보안성 제공을 제안하였다.



[그림 4] STA가 AP1에서 AP2로 이동했을 경우

제안된 메시지 전달 방법을 간단한 동작과정그림과 시퀀스 다이어그램으로 설명하면 다음과 같다.



[그림 5] STA가 AP1에서 AP2로 이동시 메시지 이동

먼저, STA은 새로운 AP인 AP2내의 영역에 들어가게 되면 AP2의 주기적 브로드캐스팅 beacon메시지를 수신하여 해당 파라미터를 참조해서 Re-association Request 메시지를 AP2에게 보내게 되고 AP2는 STA에게 이에 대한 응답으로 Re-association Response 메시지를 보낸다. 이때 STA은 이미 AP2로부터 수신한 beacon 메시지에 포함된 AP2의 IP Address를 얻을 수 있고, Move-Request 메시지를 AP2의 IP Address 주소와 함께 공개키를 이용하여 암호화해서 Key-Request 메시지에 실어 AP1에게 보낸다. 메시지를 받은 AP1은 이에 대한 응답으로 Move-response 메시지를 AP2의 IP Address와 함께 Key-Response 메시지에 실어 인증서버에게 보내면 이를 받은 인증서버는 AP2로부터 받은 Access-request 메시지와 AP1 으로부터 받은 메시지를 검사 후, 인증에 성공했을 경우 AP2에게Access-accept 메시지를 보낸다. 이로써 새로운 AP인 AP2는 인증되어지고 이전의 AP인 AP1 으로부터 WEP 키를 획득할 수 있게 된다. 이로써 공개키를 이용한 좀 더 높은 수준의 보안을 이루며 또한 STA이 두 AP를 인지하여 접속시킴으로써 두 AP간의 연결성을 높인다.

5. 결 론

본 논문에서는, Old AP 와 New AP 사이에서 주고받는 Security 정보와 WEP 키 누출을 방지하기 위해서, 메시지 경로를 이미 인증되어 사용되어졌던 경로로 바꾸고 또한 좀 더 높은 보안성을 위해 공개키를 이용하여 Security 정보를 보호하는 방법을 제안하였다. 이를 통해 악의적 공격용 소스에 의한 WEP 키 유출에 대한 방지가 기대된다.

참고 문헌

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

[2] IEEE 802.11b, "Wireless LAN Medium Access control (MAC) and Physical Layer (PHY) specification", 1999.

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

[4] IEEE 802.11f/D3.0 (Draft Supplement to IEEE 802.11, Edition): "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation".

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

[6] IEEE Draft P802.1X/D11, "Standard for Port based Network Access Control," IEEE, Mar. 2001.