무선 LAN 환경에서 단말 이동시 전송되는 AP간 WEP 키 전송 개선 방안

송 일 규[†] · 홍 충 선[††] · 이 대 영[†††]

요 약

무선LAN(wireless Local Area Network)이란 옥내 또는 옥외 환경에서 무선으로 네트워크 환경을 구축하는 것을 말하며, 기술적인 측면에서는 허브(Hub)에서 PC(Personal Computer), 노트북PC, PDA 등 클라이언트까지 유선 대신 전파나 빛을 이용하여 네트워크를 구축하는 방식을 말한다. 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 연결성을 제공한다. 본 논문에서는 위의 AP간 메시지 전달시 발생할 수 있는 보안성이 요구되는 iapp-move 요청, 응답 메시지를 이미 사용되고 있는 인증된 경로를 통해 전달함으로써 WEP키 등의 보안성이 요구되는 정보의 유출을 막고, 무선구간의 보안성을 제공하기 위해 공개키를 이용한 방안을 제시하고자 한다.

Improvement of WEP Key transmission between APs during STA Movement in Wireless Environment

Il-Gyu Song[†] · Choong-Seon Hong[††] · Dae Young Lee[†††]

ABSTRACT

Wireless LAN(wireless Local Area Network) is constructed network environment by radio in indoors or outdoors environment and that to use electric wave or light instead of wire to client such as PC(Personal Computer), notebook, PDA in hub(Hub) in technological side. Now, among IEEE 802.11 WG(Working Group), there is TGf(Task Group F) that develop standard protocol between AP's(Access Point). In this group, proposed IAPP(Inter Access Point Protocol) to secure interoperability between AP producing in different manufacturer, this offers seamless connectivity between STA by sharing Security Context information or Layer 2 forwarding information between AP without passing through re-authentication process when STAs(Station) move by protocol to secure mobility between AP that differ in equal serve network. In this paper, I wish to suggest method that change avenue of communication of message to block information leakage that can occur at security message or WEP Key transmission between above AP, and uses public key to offer wireless area security little more.

키워드 : 무선 LAN(Wireless LAN), IAPP, 로밍(Roaming), 인증(Authentication), 네트워크 보안(Network Security)

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 업체별 AP 설계에 유연성과 다양성을 주었지만 이로 인해 AP간의 상호연동이 어렵게 되었다. 이러한 문제를 해결하기 위해 TGf에서는 업체들 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. 더욱이 무선 매체는 공개성을 특성으로 하고 있기 때문에 무선 매체를 관리하는 AP 사이의 상호 연동을 수행하기 위해서는 보안 체계의 확립이 필수적으로 이루어져야 한다. IAPP에서는 AP간의 보안성이 요구되는 정보의 보안을 위해서 ESP(IP Encap-

※ 본 연구는 University ITRC 프로젝트 지원에 의해 수행되었음.
† 준 회 원 : 경희대학교 대학원 전자공학과
†† 종신회원 : 경희대학교 전자정보학부 교수
††† 정 회 원 : 경희대학교 전자정보학부 교수
논문접수 : 2003년 10월 13일, 심사완료 : 2004년 2월 26일

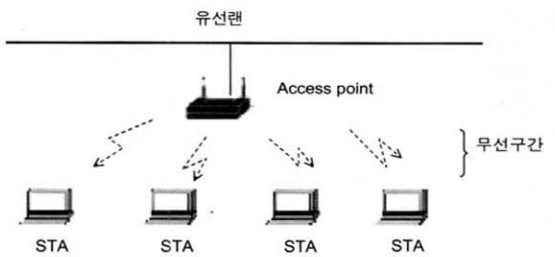
sulating Security Payload)[5]를 이용하고 있지만, 근래에 들어서 키 유출에 관한 문제점들이 많이 발생하고 있다.

본 논문에서는 단말의 신속한 이동을 지원하기 위한 AP간 정보의 공유시 발생할 수 있는 정보유출을 막기 위해 공유정보의 이동경로를 바꾸고 무선구간의 키 전송시 필요한 보안을 위해 공개키를 이용한 방법을 제안하였다. 본 논문의 구성은 다음과 같다. 제2장에서는 관련연구로서 무선 LAN의 소개와 특징을 설명하고 제3장에서는 802.11b의 기본적 인증방법을 소개하며, 제4장에서는 기존의 IAPP 프로토콜의 구조와 동작에 대해 알아보며, 제5장에서는 AP간의 공유정보의 전달에 있어서의 메시지 보안에 관한 방법을 제안하고 이에 대한 성능평가를 보여주며, 마지막으로 제6장에서는 결론을 맺는다.

2. 관련 연구

2.1 무선LAN의 개념 및 특징

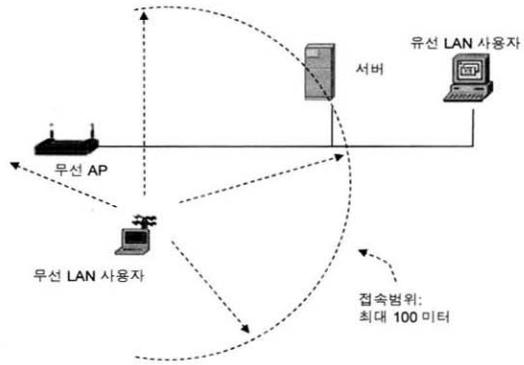
일반적으로 무선 LAN(Wireless Local Area Network)이란 사무실, 상가, 가정, 등 옥내 또는 옥외 환경에서 무선으로 네트워크 환경을 구축하는 것을 말하는데, 즉 클라이언트까지 유선대신 전파나 빛을 이용하여 무선으로 네트워크를 구축하는 방식이다. 현재 무선 LAN은 IEEE(Institute of Electrical and Electronic Engineers) 표준화 활동과 관계가 크다. IEEE 802.11 작업반(Working Group)은 1990년 7월에 무선 매체 접근 제어(MAC : Medium Access Control)를 포함한 무선 LAN 표준안 작성을 위해 승인되었다.



(그림 1) 무선 LAN의 Infrastructure 방식

IEEE 802.11 표준에 근거한 무선LAN은 무선이라는 특징을 제외하고는 사용자 또는 소프트웨어 개발자 입장에서는 이더넷을 기반으로 하는 유선 LAN의 확장 개념이라 할 수 있다. AP(Access Point)는 LAN의 허브와 유사한 역할을 수행하며, 한개의 AP당 반경 20~150m 정도의 영역에서 동시에 25~50개의 무선 NIC(Network Interface Card)가 장착된 단말을 접속하여 사용할 수 있다. 기본적인 네트워크 토폴로지로서 다수의 무선 LAN 단말끼리 독립적으로 연결하는 애드혹(Ad-hoc) 망과 AP를 통해 유선LAN에 연결하는 인프라스트럭쳐(Infrastructure) 방식이 있고, 또한 AP간에는 로밍(Roaming)에 의해 단말의 이동이 가능하다.

무선 네트워크 접속 구역은 무선 네트워크 서비스 구역을 의미한다. 유선 네트워크와는 달리 무선 사용자는 네트워크에 접속하기 위해 특정 위치에 있어야 할 필요가 없다. AP와 통신을 하기에 충분한 전파 강도와 서비스를 받을 권한이 있는 사용자는 네트워크 서비스 구역 안에 있으면 네트워크에 접속할 수 있다. 아래 그림은 무선 접속 개념을 보여주고 있다.



(그림 2) 무선접속

앞에서도 언급한 것처럼 무선랜이 초기에 널리 퍼지지 않은 원인은 표준이 없었기 때문이었다. 업체들만의 독특한 제품을 만들어야 경쟁에서 이기기 때문에 독점적이지 못한 표준을 받아들일지는 문제점으로 남을 수 있다. 비록 802.11이 물리계층, MAC, 주파수, 전송률 등에 대한 표준을 제시하지만 모든 업체들의 제품이 이를 준수한다고 보장할 수는 없다. 일부 업체는 기존 고객을 지원하기 위해 802.11 제품에서도 작동하는 방식으로 상호작용을 지원하고 있다. 다른 업체들은 802.11 제품에 업체만의 확장가능을 도입하기도 했다. 사용자가 802.11과 상호 작동하는 무선 네트워크를 구성하는 것을 보장하기 위해서 WECA(Wireless Ethernet Compatibility Alliance)가 802.11 장비를 테스트하고 증명서를 부여한다. 승인을 받았다는 증명서는 특정 장비가 다른 장비와의 상호작용에 관한 엄격한 시험을 통과했으므로 소비자는 이를 안심하고 사용해도 된다는 것을 의미한다. 이미 구축된 네트워크에 새로운 장비를 도입할 경우 이런 문제가 매우 중요하다. 왜냐하면 만약 장비가 서로 통신할 수 없다면 네트워크 운영이 매우 복잡해지며, 서로 다른 네트워크를 운영해야만 하기 때문이다.

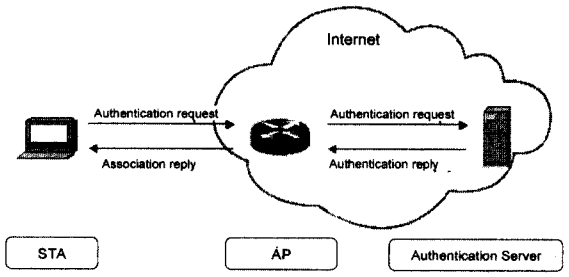
802.11 표준이 1997년에 승인되었기 때문에 개선을 위해 여러 차례 제안이 있었다. 현재 우리나라에서 사용되고 있는 802.11b 표준은 이제는 5배 대역폭을 지원하는 802.11a[7]가 개발되어 사용되고 있고, 802.11g도 조만간 나올 예정이다.

무선LAN을 구축할 때 네트워크 관리자가 직면하는 가장 큰 걱정거리는 보안이다. 유선 네트워크 환경에선 물리적 회선의 연결 부족으로 내부 네트워크에 연결하는 것을 방지할 수 있다. 무선 랜의 경우 무선 기기를 사용하고 있는 사람이 건물 안에 있는지, 로비에 있는지 혹은 건물 밖에 있는지 알아낼 수 없다. IEEE 802.11에서는 신뢰할 수 없는 전파를 통해 데이터를 전송하는 것이 결국에는 스누핑을 유발한다는 것을 알고 있으므로 무선 랜을 통과하는 데이터의 보안을 증대하기 위해 3가지 방법을 도입했다.

첫번째 방법은 802.11 SSID를 사용하는 것이고, 두번째 방법이 MAC 주소에 근거하여 무선기기를 인증하는 것이며, 세번째 방법이 WEP 키를 사용하는 것이다. MAC주소를 이용한 방법은 AP내부에 저장되어있는 리스트나 혹은 외부 데이터베이스에 저장되어 있는 리스트를 보고 인증요청이 오면 이를 이용하는 것으로 리스트의 내용과 비교하여 인증을 이루는 방법이다. 즉 저장되어있는 리스트의 내용에 부합되는 사용자만이 인증에 성공하는 방법이다. 이러한 방법은 작은 사이즈의 무선 네트워크에서 유리하다. SSID와 WEP은 다음 장에서 구체적으로 설명하겠다.

2.2 802.11b의 기본적인 인증방법

최근 많이 사용되고 있는 IEEE 802.11b 무선랜 보안 기술[11]을 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 인증 서버를 이용하여 STA에게 접속을 하게 된다. 접속과정은 (그림 3)과 같다.



(그림 3) STA 사용자의 네트워크 접속과정

현재 사용되고 있는 802.11b 표준은 무선랜의 인증과정과 비밀성을 제공하기 위해 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. SSID는 무선LAN에서 논리적으로 영역을 분할하는 의미로 사용하는 번호이고, 보안측면에서는 아주 취약하므로 SSID만을 사용하여 무선LAN을 구축하게 되면 많은 문제가 발생할 수 있다.

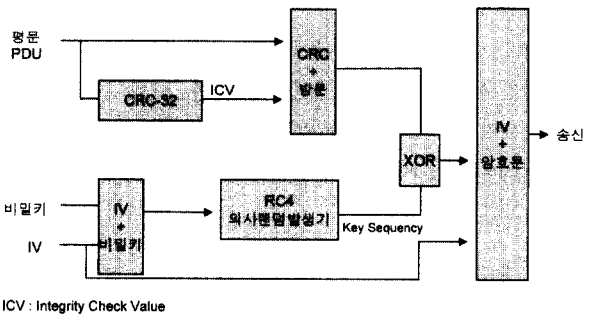
SSID를 사용한 접속제어는 처음 접속시 단말에서 송신한 Probe 요청메시지에 대한 응답인 프루브(Prove) 응답메시지에 실려 오거나 또는 액세스포인트에서 주기적으로 브로드케스팅 하는 비콘 메시지에 포함되어 있다. 이 메시지 내에 들어있는 SSID를 이용하여 단말에서 접속을 시도하고 인지함으로써 기본적이 접속제어가 이루어지고 이를 통해 기본적인 인증 과정이 이루어지는 것이다.

SSID는 인프라스트럭처 BSS(Basic Service Set)에 여러 개의 무선 랜 세그먼트를 만들기 위해 하나 이상의 AP와 관련이 있다. 세그먼트란 빌딩의 층 또는 업무 단위 및 데이터정의 셋과 관련이 있다. SSID는 인증과정에서 나타나므로 원상태 그대로의 패스워드로 작동하게 된다. 대부분 최종사용자가 무선기기를 설정하므로 SSID는 사용자들 간에 공유되며 이로 인해 보안의 효율이 떨어진다.

인증 방법으로 SSID를 사용하는데 따른 또 하나의 불편한 점은 만약 SSID가 변경된 경우 모든 무선기기 및 AP의 SSID를 변경해야 한다는 단점이 있다.

보안의 효율이 떨어지는 SSID를 기반으로 하는 방안은 효율이 떨어지므로, 추가적으로 데이터에 대한 보안성을 제공하기 위하여 WEP(Wired Privacy Equivalent) 방식의 암호화를 병행하면서 좀더 강도 높은 보안을 제공한다.

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.



(그림 4) WEP 방식 암호화 과정

WEP 방식의 암호화 과정에 대한 주요한 5개 요소를 보면 다음과 같다.

① 공유키 : 모든 BSS 멤버스테이션이 공유하는 값

② 암호화 알고리즘 : RC4 스트림 암호화 알고리즘으로서, 공유키와 IV로부터 키스트림을 생성시킨다. 이 키값은

평문을 XOR 연산하여 암호문으로 만들기 위하여 사용된다. 복호시에도 같은 알고리즘을 사용한다.

③ 24비트 IV(Initialization Vector) : 공유키에 덧붙여져 RC4 암호화되어 새로운 키 스트림을 생성한다. WEP가 매 패킷을 보낼 때마다 새로운 IV 값을 선택한다.

④ 캡슐화 : 송신기에서 수신기로 전송하기 위하여 암호문에 IV를 덧붙인다.

⑤ 무결성 알고리즘 CRC-32 : CRC는 페이로드 데이터로부터 연산되어 그 페이로드에 덧붙여진 후 암호화 된다.

그러나 이 방법은 다소의 문제점이 있다. 동일한 암호키, 복호키, 또한 이 알고리즘을 단말과 액세스포인트가 공유하여 운용하는 방법이므로 이 경우 키 분산시 관리가 어려워지고, 키 공유에도 어려움이 있다. 정적으로 키가 관리되기 때문에 키 분배 적용이 어렵고 보안성이 낮아지는 단점이 있다. 이를 해결하기 위해 IEEE802.11i[8] 그룹에서는 기존의 WEP키의 길이를 길게 하여 보안강도를 향상시킨 WEP 2등이 보완책으로 있고 RSN(Robust Security Network)을 이용하는 방법 등이 제시되고 있다.

액세스포인트와 인증 서버 사이의 보안을 위해서 RADIU 프로토콜을 사용하게 되는데, 이는 NAS(Network Access Server)와 인증 서버사이에 인증, 서비스 허가, 과금에 관한 정보전달을 위한 프로토콜로써, 유선 환경에서 로밍 PPP (Point to Point Protocol)사용자를 인증하기 위한 AAA(Authentication, Authorization, Accounting) 프레임워크로 제안되었다. RADIUS서버는 사용자의 연결 요구에 대해 사용자 인증을 해주고, 액세스포인트는 인증 받은 사용자에게 허가된 서비스를 제공한다.

2.3 공개키

공개키는 지정된 인증기관에 의해 제공되는 키 값으로서, 이 공개키로부터 생성된 개인키와 함께 결합되어, 메시지 및 전자서명의 암호화와 복원에 효과적으로 사용될 수 있다. 공개키와 개인키를 결합하는 방식은 비대칭 암호작성법으로 알려져 있다.

2.3.1 PKI(Public Key Infrastructure)

PKI는 기본적으로 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이, 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해준다. PKI는 한 개인이나 기관을 식별할 수 있는 디지털 인증서와, 인증서를 저장했다가 필요할 때 불러다 쓸 수 있는 디렉토리 서비스를 제공한다. 비록 PKI의 구성 요소들이 일반적으로 알려져 있지만, 공급자 별로 많은 수의 서로 다른 접근방식이나 서비스들이 생겨나고 있으며, 그동안에도 PKI를 위한 인터넷 표준은 계속하여 작업이 진행되었다.

PKI는 인터넷 상에서 메시지 송신자를 인증하거나 메시지를 암호화하는데 있어 가장 보편적인 방법인 공개키 암호문을 사용한다. 전통적인 암호문은 대개 메시지의 암호화하고 해독하는데 사용되는 비밀키를 만들고, 또 공유하는 일들이 관여된다. 이러한 비밀키나 개인키 시스템은, 만약 그 키를 다른 사람들이 알게 되거나 도중에 가로채어질 경우, 메시지가 쉽게 해독될 수 있다는 치명적인 약점을 가지고 있다. 이러한 이유 때문에, 인터넷 상에서는 공개키 암호화와 PKI 방식이 선호되고 있는 것이다(개인키 시스템은 때로 대칭 암호작성법, 그리고 공개키 시스템은 비대칭 암호작성법이라고도 불린다).

PKI는 다음과 같은 것들로 구성된다.

- 디지털 인증서를 발급하고 검증하는 인증기관
- 공개키 또는 공개키에 관한 정보를 포함하고 있는 인증서
- 디지털 인증서가 신청자에게 발급되기 전에 인증기관의 입증을 대행하는 등록기관
- 공개키를 가진 인증서들이 보관되고 있는 하나 이상의 디렉토리
- 인증서 관리 시스템

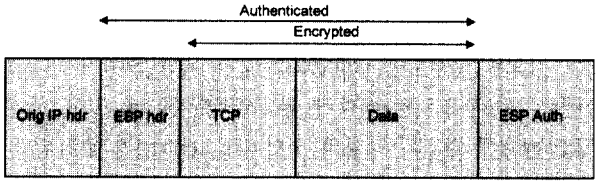
2.3.2 공개키와 개인키 암호화의 동작원리

공개키 암호화에서, 공개키와 개인키는 인증기관에 의해 같은 알고리즘(흔히 RSA라고 알려져 있다)을 사용하여 동시에 만들어진다. 개인키는 요청자 에게만 주어지며, 공개키는 모든 사람이 접근할 수 있는 디렉토리에 디지털 인증서의 일부로서 공개된다. 개인키는 절대로 다른 사람과 공유되거나 인터넷을 통해 전송되지 않는다. 사용자는 누군가가 공개 디렉토리에서 찾은 자신의 공개키를 이용해 암호화한 텍스트를 해독하기 위해 개인키를 사용한다. 만약 자신이 누구에겐가 어떤 메시지를 보낸다면, 우선 수신자의 공개키를 중앙 관리자를 통해 찾은 다음, 그 공개키를 사용하여 메시지를 암호화하여 보낸다. 그 메시지를 수신한 사람은, 그것을 자신의 개인키를 이용하여 해독한다. 메시지를 암호화하는 것 외에도, 송신자는 자신의 개인키를 사용하여 디지털 인증서를 암호화하여 함께 보냄으로써, 메시지를 보낸 사람이 틀림없이 송신자 본인이라는 것을 알 수 있게 한다.

2.4 ESP 동작 개요

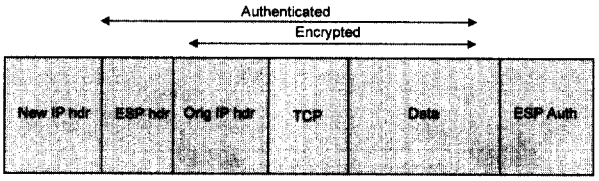
ESP는 기밀성, 원본 데이터의 인증, 무결성과 같은 보안 서비스를 지원하기 위하여 설계된 프로토콜로 IP 데이터그램 안에 삽입된다. IP 데이터 그램 안에 ESP가 삽입될 경

우 ESP 뒤의 데이터는 암호화 된다. 그리고 수신측 에서는 IKE로 미리 교환한 키값을 이용하여 데이터를 복호화 하는 기능을 수행하게 된다. ESP 모드에는 크게 전송모드(Transport mode)와 터널모드(Tunnel mode)가 있다.



(그림 5) Transport 모드

전송(Transport)모드의 경우 ESP 헤더가 IP 헤더 뒤에 오는 경우로서 TCP 헤더와 그 뒷단의 데이터에 대한 Security를 보장해 준다. 하지만 IP 헤더가 암호화가 되지 않기 때문에 헤더정보에 대한 보안을 할 수 없다.



(그림 6) Tunnel 모드

터널(Tunnel)모드의 경우 IP 헤더까지 암호화가 되는데 이는 New IP Header라는 새로운 IP 헤더를 붙임으로써 원본 IP 헤더부터 데이터까지 암호화 되어 전송함으로 전송(Transport)모드에 비해 좀 더 안전하다.

2.5 RADIUS 프로토콜

현재 통신 장비들의 인증을 제공하기 위해 가장 널리 알려지고 많이 사용되는 프로토콜로 RADIUS(Remote Access Dial-In User Service)가 있다. 이는 1990년대 중반에 Livingston Enterprise에 의해 자사의 NAS 장비에 인증과 과금 서비스를 제공하기 위해 개발되었다. 그후 IETF RADIUS 워킹그룹에서 1996년에 표준화 작업을 하여 프로토콜 기본 기능과 메시지 형식이 RFC 2138로 문서화 되었다. RADIUS의 기능 속성을 간단히 설명하면 다음과 같다.

① 클라이언트-서버 기반의 동작 : RADIUS 클라이언트는 NAS에 있고 네트워크를 통해 호스트 컴퓨터에서 운영되는 RADIUS 서버와 통신한다. 또한 RADIUS 서버도 다른 RADIUS나 인증 서버에 대해 프록시 클라이언트로 동작할 수 있다.

② 네트워크 보안 : RADIUS 클라이언트와 서버 사이의 모든 통신은 네트워크를 통해 전달되지 않는 공유 비밀키에 의해 인증 된다. 또한 RADIUS 메시지 안에 포함되어 있는 사용자 비밀번호는 해커의 공격으로부터 보호하기 위해 암호화 된다.

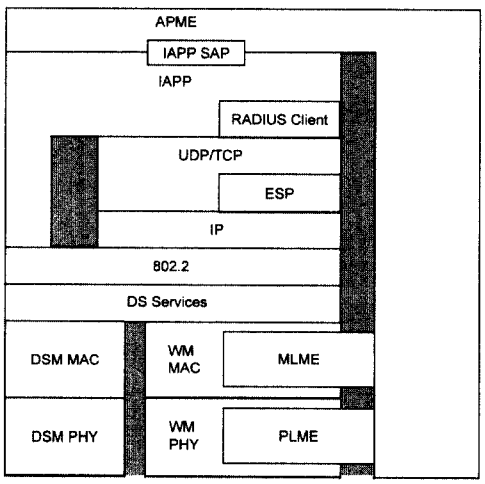
③ 유연한 인증 : RADIUS는 인증을 위해 PAP, CHAP 등 다양한 인증 방법을 지원한다.

④ Attribute/Value 쌍 : RADIUS 메시지들은 Attribute 또는 Attribute/Value쌍이라 불리는 Type-Length-Value 필드로 인코딩되어 AAA[9] 정보를 실어 나른다.

3. IAPP 프로토콜

3.1 IAPP 프로토콜의 구조

IAPP는 AP의 특성과 기능을 구현하고 있는 AP 운영 엔티티인 APME(AP Management Entity)와 IAPP SAP(Service Access Point)를 통해 IAPP-INITIATE 서비스 프리미티브를 교환하며 초기화된다. IAPP는 APME를 통해 STA 재설정 요청을 수신한 경우 802.1X 인증을[6] 지원하기 위해 클라이언트를 사용한다. RADIUS 클라이언트는 RADIUS 서버와 통신을 함으로써 AP의 BSSID와 IP주소를 매핑하는 기능과 AP들 사이의 암호화를 위한 키 분배 기능을 한다.



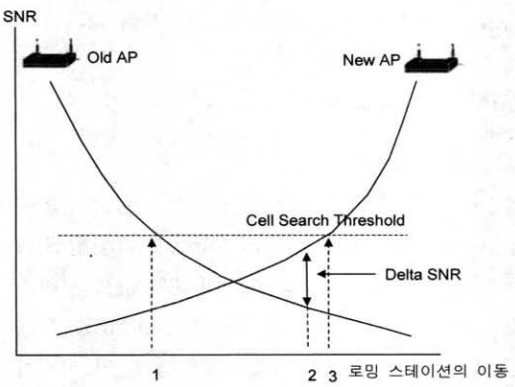
(그림 7) IAPP 구조도

- 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

3.2 무선단말의 로밍과정

무선이동단말은 SNR값을 수신하여, 현재 연결된 SNR 값과 비교를 함으로써 로밍을 하게 된다. 이때 신호레벨은 모든 AP에서 발생되는 비콘(beacon)메시지에 의해 얻어진다.

SNR값은 'Cell Search Threshold'라고도 불리는데, 이 값이 임계값(threshold value)보다 떨어지면 재연결(re-association)절차가 시작된다. 즉 현재 연결된 SNR값과 수신된 SNR값을 비교하여, 이 값의 차이가 Delta SNR로 알려진 임계값보다 크면 무선이동단말은 새로운 AP에 대해 재연결 절차를 시작하게 된다.



(그림 8) 단말의 로밍 시점

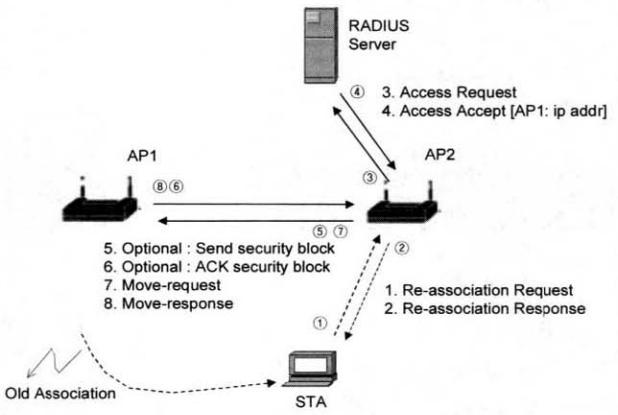
위의 (그림 8)은 무선 이동 단말의 로밍 결정에 대한 SNR 비교표이다. SNR값은 두 AP로부터 주어진 위치에서 얻을 수 있다. 만약 무선이동단말이 오른쪽으로 이동하면, 이전 AP의 SNR값은 줄어든다. 동시에 새로운 AP에 더욱 가까워지고, SNR값은 커진다. SNR값이 Cell Search Threshold 보다 떨어지면, 무선이동단말은 Cell Search 상태로 들어가며, active 채널을 찾으려고 검색에 들어간다. 오른쪽으로 더 움직이면 SNR값은 새로운 AP가 이전 AP보다 더 커지게 된다. 하지만 새로운 AP로의 연결은 이루어지지 않는다. 새로운 AP오 k이전 AP간의 SNR값의 차이가 Delta SNR 값보다 커지면 그때 로밍이 시작된다. SNR값이 Cell Search Threshold보다 커질 때까지는 Cell Search상태로 유지되며, 반대방향으로의 이동은 새로운 AP에서 이전의 AP로의 이동은 같은 절차를 갖는다.

3.3 IAPP 동작개요

동일 서브네트워크에서 서로 다른 AP간에 이동성을 보장하기 위한 프로토콜인 IAPP는 AP간 Layer 2 Forwarding 정보와 Security Context 정보를 공유함으로써 단말의 빠른 이동성을 제공한다. IAPP는 복수의 AP와 이동 스테이션, 분산시스템(DS), 그리고 하나 이상의 RADIUS서버를 포함하는 환경에서 동작한다.

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 9)와 같다. STA이 AP2 영역에 들어가게 되면, AP2에게 재설정을 요청한다. 만약 AP2가 Proactive Caching[10]을 이용하게 된다면, 우선 APME는 단말의 MAC 주소를 이용하여 IAPP의 캐쉬에 있는 단말들의 context 정보들을 찾게 된다. 이때 캐쉬의 내용에 단말의 정보와 부합되는 context를 찾게 되면 캐쉬의 내용을 곧바로 사용함으로써 빠르게 핸드오프를 할 수 있다. 또한 IAPP 캐쉬에 단말의 정보와 부합되는 context가 없다면 기존 방법대로 (그림 9)처럼 핸드오프 과정을 거치게 된다. 여기서 RADIUS Access accept메시지의 정보에는 AP1과 AP2 사이에 주고받는 Move-요청과 Move-응답 메시지를 암호화하기 위한 알고리즘인 ESP authenticator 등이 포함된다.



(그림 9) IAPP 동작 과정

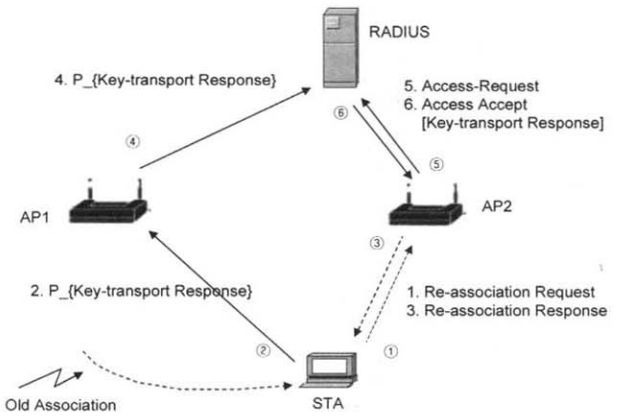
최근에 들어서 AP1과 AP2 사이에 전달되는 메시지와, STA과 AP간 Privacy를 위해 사용되는 WEP 키와 비밀번호 등이 악의적인 공격용 소스 등에 의해 노출될 위험성이 커지고 있다.

4. 제안 및 해결방안

4.1 제안사항

본 논문에서는 Old AP(AP1)와 New AP(AP2) 사이에 주고 받는 보안성이 요구되는 정보의 유출 가능성을 줄이고, IAPP가 지원되는 AP와 지원되지 않는 AP 간의 좋지 못한 연결성문제를 해결하기 위해 AP1과 AP2 사이의 메시지 전송경로를 AP1과 인증서버사이의 이미 인증되어 사용되었던 경로를 이용하고, 또한 무선구간의 보안 향상을 위해 공개키를 이용하여 보안성 향상방안을 제안하였다.

제안된 메시지 전달 방법을 간단한 동작과정 그림으로 설명하면 다음과 같다.



(그림 10) STA가 AP1에서 AP2로 이동

먼저, STA는 새로운 AP인 AP2내의 영역에 들어가게 되면 AP2의 주기적 브로드캐스팅 비콘(Beacon)메시지를 수신하여 해당 파라미터를 참조해서 재설정 요청 메시지를 AP2에게 보내게 된다. AP2는 STA에게 이에 대한 응답으로 재설정 응답 메시지를 보낸다. 이때 STA은 AP2로부터 수신한 비콘 메시지에 포함된 AP2의 프리픽스(Prefix) 정보를 이용하여 AP2를 식별하고, 기존 Move-요청 메시지에 상응하는 Key-요청 메시지를 AP1에게 보낸다. 메시지를 받은 AP1은 이에 대한 응답으로 기존 Move-응답 메시지와 같은 기능을 갖는 Key-transport 응답 메시지를 인증서버에게 보내면 이를 받은 인증서버는 AP2에게 Access-accept 메시지를 보낸다. 이때 이 Access-accept 메시지에는 Key-transport 응답 메시지가 담겨있고, 이 메시지를 받은 새로운 AP인 AP2는 인증되어지고 이전의 AP인 AP1 으로부터 WEP 키를 획득할 수 있게 된다. 만약 AP2가 2번 메시지(Key transport request)에 대한 응답메시지 수신 실패시에는 일반적인 패킷 재전송 방법처럼 수차례 재시도 후에 그래도 수신 불능 상태가 되면, 최초의 재인증 작업과 마찬가지로 새로운 인증절차를 거치게 된다.

STA과 AP 사이의 무선구간의 보안성을 위해 공개키를 사용하는데, 이때 사용되는 공개키는 최초의 인증작업을 거칠 때 인증서버와 서로 주고받은 인증서에 포함되어 획득한 공개키를 사용하게 되므로 따로 공개키를 얻을 필요는 없다. 이로써 공개키를 이용한 무선구간의 보안을 이루며 STA이 두 AP를 인지하여 접속시킴으로써 두 AP간의 연결성을 높인다.

본 논문에서는 공개키를 사용한다는 점 보다는 인증되어진 경로를 이용하여 보안성이 요구되는 메시지와 키를 전송함으로써 해커들에 의한 메시지 유출을 막고자 제안된 방법이다. 이러한 방법을 이용한다면, 현재 Draft 5.0에서 새롭게 제안된 Proactive 캐싱 방법을 사용한 것과 비슷한 성능을 나타낼 수 있고, 그렇게 함으로써 AP에게 부담이 되는 캐쉬작업을 줄여 줄 수 있다.

이러한 제안사항을 위하여 기존에 정의되어진 패킷에서 명령필드에 7번과 8번에 새로이 제안된 메시지 형식 (그림 12), (그림 13)을 삽입하여 정의하였다.

Version	Command	Identifier	Length	Data
Octet : 1	1	2	2	0 - n

(그림 11) IAPP Packet Format

Address Length	Reserved	MAC Address	Sequence Number	Length of Context Block	Context Block
Octet : 1	1	n = Address Length	2	2	m = Length of Context Block

(그림 12) Key-transport Request

Address Length	Status	MAC Address	Sequence Number	Length of Context Block	Context Block
Octet : 1	1	n = Address Length	2	2	m = Length of Context Block

(그림 13) Key-transport Response

현재 명령필드는 4번까지 정의되어져 있었고, draft 5.0에서부터 5번 6번이 새로이 정의되어졌다. 나머지 7번부터 255번까지는 예약영역으로 되어있다. 이에 7번에는 key-transport 요청메시지를 정의했고, 8번에 key-transport 응답메시지를 정의했다. 또한 RADIUS Access-Accept 메시지에 Key-transport 응답을 넣기 위해 개발자들을 위해 예약시켜놓은 RADIUS Access-Accept Attribute의 192번~223번 중에서 192번에 (그림 16)과 같이 Key-transport 응답메시지를 할당하였다.

Value	Command
0	ADD-motify
1	Move-notity
2	Move-response
3	Send-Security-Block
4	ACK-Security-Block
5	CACHE-notify
6	CACHE-response
7	Key-transport-request
8	Key-transport-response
9 ~ 255	Reserved

(그림 14) Command field value

Code	Identifier	Length	Response Authenticator	Attributes
Octet : 1	1	2	3	n

Code	Assigned
1	Access-Request
2	Access-Accept
3	Access-Reject
	...
14 ~ 255	Reserved

(그림 15) RADIUS data format

Attribute number	Attribute Name	Value
1	User Name	Old BSSID
8	Frame IP Address	Old BSSID IP Address
...	...	...
80	Message-Authenticator	RADIUS Message's Authenticator
192	Key-transport	Key-transport response

(Value 192~133 are reserved for esperimental use)

(그림 16) RADIUS Access-Accept Attribute

4.2 측정 결과

이 논문의 목적은 WEP키 등의 보안성이 요구되는 메시지의 전송경로를 우회하여 최소한으로 메시지 유출을 막고자 하는 논문이므로 전체적 성능평가를 측정하여 안전경로로 우회 하였을 때에 전체적 delay 측정을 하여, 사용타당성 여부를 평가하고자 한다.

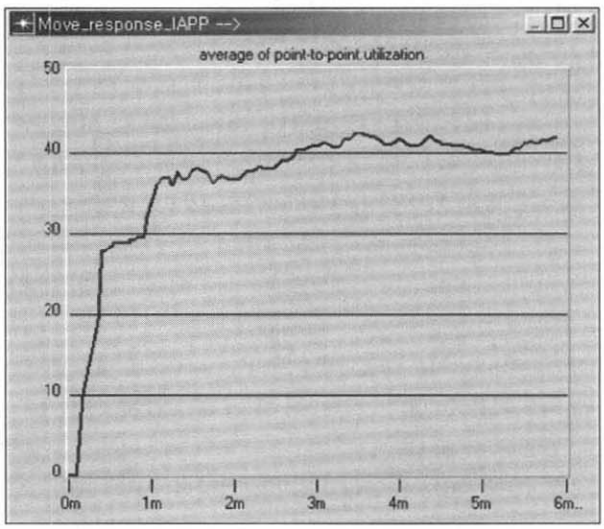
시뮬레이션을 위한 환경설정 및 결과를 보면 다음과 같다. 컴퓨터 환경은 PentiumIII 800 CPU를 탑제한 Windows2000 운영체제의 컴퓨터에서 OPNET8.0 시뮬레이터를 이용하여 시뮬레이션을 하였다.

먼저 대역폭 사용률 체크를 위한 Utilization과 전체적 성능평가를 위한 End-to-End 지연(Delay)을 측정하였는데, 그 결과는 아래 그림과 같다.

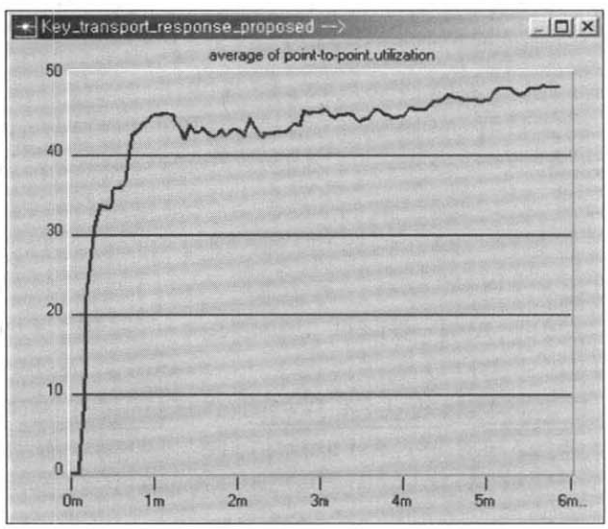
〈표 1〉 시뮬레이션 환경설정

Network	Bandwidth	Delay	통신속도
LAN	10Mbps	5ms	9600bps
Wireless	1Mbps	20ms	9600bps

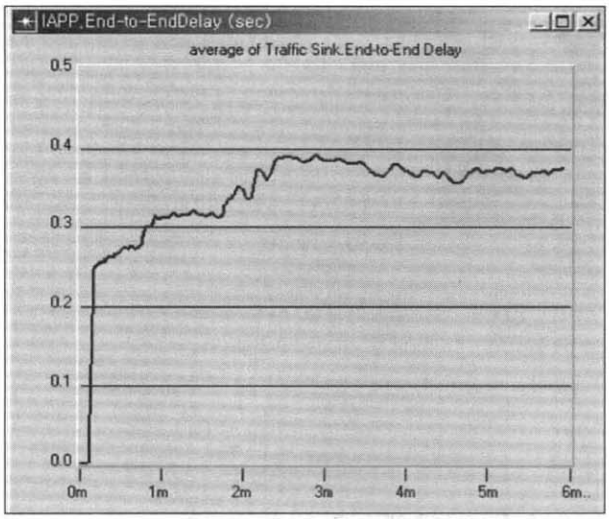
시뮬레이션 측정 결과를 보면, 본 논문에서 제안한 방법은 Move-요청 메시지를 전송하기 위해 재설정 요청메시지를 보냄과 동시에 Move-요청 메시지와 같은 기능을 갖는 Key-transport 요청 메시지를 보냄으로써 좀 더 빠르게 WEP Key를 받을 수 있다. 하지만 위의 제안사항은 기존의 IAPP 방식보다 통신성능평가는 조금 떨어진다. End-to-End Delay 측정의 경우 매 msec 당 최소 0.03에서 최대 0.07의 지연을 보이고 있음을 알 수 있다. 이는 공개키 사용으로 인한 프로토콜 전반의 오버헤드로 분석된다. 하지만 두 AP 사이에서의 메시지 전송 중에 생길 수 있는 해커들에 의한 메시지 캡처링을 막을 수 있으며, STA과 AP의 무선구간 사이에서의 키 전송시 공개키를 이용하여 보안성을 제공한다는 장점이 있다.



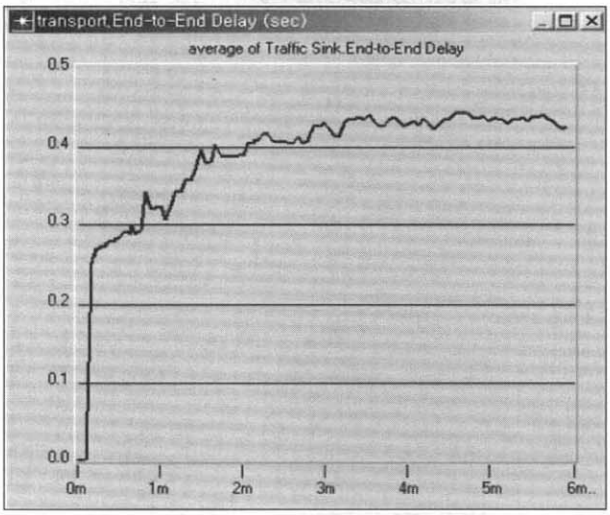
(그림 17) Utilization 측정(기존)



(그림 18) Utilization 측정(제안)



(그림 19) End-to-End Delay 측정(기존)



(그림 20) End-to-End Delay 측정(제안)

〈표 2〉 기존 IAPP와 제안구조의 특성비교

	기존 IAPP	제 안
AP 사이에서의 메시지 전송	두 AP 사이에서의 데이터 캡처링에 취약	AP 사이에서의 데이터 전송을 없애고 인증키를 안전한 경로로 우회함
암호와 기법	ESP 사용	공개키 사용
키 요청과 응답	Re-association에 대한 응답을 받은 후 인증키 요청	Re-association에 대한 응답을 받은 전에 인증키 요청

5. 결 론

본 논문에서는, AP1와 AP2 사이에서 주고 받는 WEP 키 및 보안성이 요구되는 정보들의 유출을 방지하기 위해서, 메시지 경로를 이미 인증되어 사용되어 지고 있는 경로로 바꾸었다. 또한 무선구간의 키 전송시 필요한 보안을 위해 공개키를 이용한 방법을 제안하였다. 이를 통해 악의적 공격용 소스에 의한 두 AP간 메시지 유출에 대한 방지가 기대된다. 또한 재설정 요청과 동시에 Key-transport 요청 메시지를 보냄으로써 좀 더 빠른 연결성을 제공할 수 있을 것이다. 802.11f/Draft 5.0에서 새롭게 추가된 Proactive 캐쉬 메커니즘을 사용하지 않고 이와 비슷한 성능을 발휘할 수 있다면 AP가 캐쉬작업에 의한 부담을 줄일 수 있다.

참 고 문 헌

[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.

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

[8] IEEE 802.11i-D2.0, "Draft-WirelessMedium Access Contro(MAC) and physical layer(PHY) specification : Specification for Enhanced security," March, 2002.

[9] Christopher Metz, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," Cisco system.

[10] IEEE802.11f/D5.0 (Draft Supplement to IEEE802.11, Edition) : "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation".

[11] D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5," IEEE, 802.11-01/400r22, July, 2001.

송 일 규

e-mail : niceguy@cvs2.kyunghee.ac.kr

2001년 경희대학교 전자공학과(학사)

2004년 경희대학교 대학원 전자공학과 (공학석사)

관심분야 : 무선인터넷보안, 무선LAN, Home Network

홍 충 선

e-mail : cshong@khu.ac.kr

1983년 경희대학교 전자공학과업(학사)

1985년 경희대학교 전자공학과(공학석사)

1997년 Keio University 정보통신전공 (공학박사)

1988년~1999년 한국통신 통신망 연구소 선임 연구원/ 네트워킹연구실장

1999년~현재 경희대학교 전자정보학부 조교수

관심분야 : 인터넷 서비스 및 망 관리, 네트워크보안, 모바일 네트워킹

이 대 영

e-mail : dylee@khu.ac.kr

1964년 서울대 물리학과(학사)

1971년 캘리포니아 주립대학원 컴퓨터학과 (공학석사)

1979년 연세대학교 전자공학과(공학박사)

1990년~1993년 경희대학교 산업정보대학원 대학원장

1999년~2000년 한국통신학회장

1971년~현재 경희대학교 전자정보학부 교수

관심분야 : 영상처리, 컴퓨터 네트워크, 컴퓨터시스템등