공중 무선랜 망에서 인증 및 키관리 기술 동향

Technology Trends on Authentication and Key Management in Public WLAN Networks

정병호(B.H. Chung) 무선인터넷보안연구팀 선임연구원, 팀장
강유성(Y.S. Kang) 무선인터넷보안연구팀 연구원
김신효(S.H. Kim) 무선인터넷보안연구팀 선임연구원
정교일(K.I. Chung) 정보보호기반연구부 책임연구원, 부장

최근 통신 사업자(WISP)들은 공항, 아파트 등 핫스팟 지역에서 무선랜을 공중 액세스망으로 이용한 초고속 무선인터넷 서비스 네트워크를 구축하고 있다. 이러한 가운데 무선랜에서의 보안 결함이 밝혀지고, 무선랜 환경에서의 개인 프라이버시 침해 문제가 사회적인 현안으로 등장하였다. 본 고에서는 무선랜 기반 공중 액세스망의 보안성 강화를 위하여 국제 표준화기구에서 논의하고 있는 가입자 인증 및 키관리 기술의 동향과 향후 전망에 대해서 분석해 보고자 한다.

I. 서 론

2001년, 3세대 이동 통신망(IMT-2000)의 전송속도가 당초 2Mbps의 기대에 미치지 못할 뿐만 아니라 고가의 통신 서비스 비용이 예상되고, 상용화 시기도 늦어지면서 무선랜이 초고속 무선인터넷의 좋은 대안이 될 수 있다는 인식이 급속히 확산되기 시작하였다. 기존의 인터넷 사업자(ISP)들은 핫스팟 지역에 무선랜을 설치하여 값싼 초고속 멀티미디어 무선인터넷 서비스를 제공하는 방향으로 유무선 통합망을 구축하고 있으며, 이동통신 사업자들 역시 이동통신과 무선랜을 연동하는 방향으로 유무선 통합망을 구축하기 위한 노력을 진행하고 있다. 이러한 유무선 통합망을 이용한 무선 인터넷 사용자들은 무선으로 이동하면서 전자메일, 상거래, VoIP 등을 초고속으로 편리하게 서비스받는 만큼, 프라이버시 정보를 보호받고 싶은 보안성 욕구도 함께 증가하고 있다. 이는 무선매체의 공개성에 따른 해킹의 용이성과 단말의 이동에 따른 보안 체계의 복잡성에 기인한다. 따라서 최근 무선랜 기반 유무선 통합망 구축시 보안성이 가장 중요한 영역으로 인식되고 있는 현실이다[1].

그러나 무선랜의 기술적인 측면에서 볼 때, 유무선 통합망 구축에는 해결되어야 할 장벽이 아직 많이 남아 있다. 정보 기술의 진화 속도가 사용자의 욕구(예를 들면 초고속, 고품질, 고보안)를 따라가지 못하는 것이다. 실험실 등 소규모 사설망 수준에서 이용되던 무선랜을 대규모 기업망 또는 공중망에서 활용하려다 보니 무선랜의 보안 결함들이 부각되기 시작하였다. 전세계적으로 가장 많이 배치되어 이용중인 802.11b 무선랜은 당초 보안에 큰 관심을 두지 않았고 또 공중망에서의 활용을 전제로 설계되지 않았던 것이 사실이다. 예를 들면, 무선랜은 브로드캐스팅 특성으로 인하여 도청 등 무선 데이터 프라이버시에 대한 취약성이 예상되었음에도 불구하고, 동적인 키분배 방법이 없다거나, 취약한 무결성 알고리듬을 사용하여 데이터 프라이버시를 제공하지 못한다는 점이다.

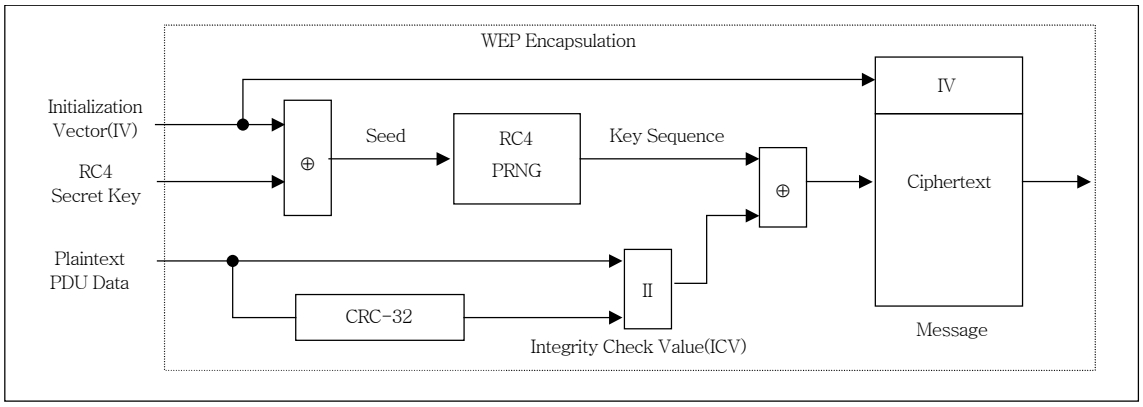
전술한 바와 같이 무선랜이 공중 액세스망에서 차지하는 비중이 점차 높아가고, Mobile-IP를 이용한 무선인터넷 서비스의 주 타깃 망이 무선랜이 될 가능성이 높아지면서 IEEE, IETF, ETSI, 3GPP, 3GPP2 등 국제 표준화 기구에서도 상호 협력하는 가운데 표준화를 진행하고 있다. 무선랜 보안의 표준을 제정하고 있는 IEEE 802.11i(Enhanced MAC security)[2] 워킹그룹은 최근 무선랜 인프라망과 Ad-Hoc 망에 적용할 수 있는 새로운 형태의 보안 아키텍처(Robust Security Network: RSN)를 제안하고 표준화를 진행하고 있다. RSN은 다수의 액세스포인트가 연결된 핫스팟에서 802.1x 기반 가입자 인증을 통한 네트워크 접속 제어, 보안 세션 관리, 패킷당 키관리, 그리고 새로운 암호 알고리듬 도입을 통한 무선 접속구간 보안을 강화하는 데 이용된다. IEEE 802.11 워킹 그룹은 최근 802.1x(port-based network access control)와 802.11i를 결합시키는 작업을 진행해왔고, RSN이 아직 미완성의 표준이지만 그 동안 지적되어 왔던 보안 문제의 상당 부분을 해결할 수 있을 것으로 판단된다.

본 고에서는 먼저 기존의 무선랜 망에서의 보안 문제점이 무엇인지를 Ⅱ장에서 정리하고, Ⅲ장에서는 802.11i WG에서 제안한 새로운 무선랜 보안(RSN) 개념을, 그리고 Ⅳ장에서는 RSN에서 보안 세션을 설정하기 위하여 단말과 액세스포인트 간에 이루어지는 보안 협상 방법에 대해서 살펴보겠다. RSN 보안 협상이 종료되면 협상 결과에 따른 인증 및 키분배 과정이 진행되고, 단말과 액세스포인트, 그리고 인증서버 간에 보안 어소시에이션이 형성되어 무선 접속구간의 보안이 강화된다. 이와 관련하여 Ⅴ장에서는 802.1x를 이용한 상호인증 및 마스터 키분배 절차에 대해서 설명하고, Ⅵ장에서 TKIP cipher suite를 이용하여 보안 어소시에이션을 형성하는 과정을 설명하겠다. 그리고 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 무선랜 보안의 문제점

유선랜에서는 물리적으로 연결된 단말들만이 랜 트래픽을 감지할 수 있다. 그러나 무선랜은 기본적으로 브로드캐스팅 망이므로, 액세스포인트의 비컨 수신 영역 내에 있는 모든 단말들은 다른 사람의 송수신 데이터 내용을 청취할 수 있다. 따라서 무선랜에서는 원하는 수신자 이외에 다른 사람이 메시지 내용을 보지 못하게 하는 데이터 프라이버시와 상호인증 서비스가 매우 중요하다. 무선랜을 통한 네트워크 접속에는 두 개의 보안구간의 정의가 필요하다. 사용자와 액세스포인트 사이의 무선 접속 구간 보안과 액세스포인트와 인증서버 사이의 유선 구간 보안이다. 현재 IEEE 802.11b 표준[3]은 WEP(Wired Equivalent Privacy) 알고리듬을 사용해서 무선 보안이 이루어지고 있다. 유선 구간에서는 RADIUS (Remote Authentication Dial In User Service)[4]나 TACACS+ (Terminal Access Controller Access Control System)[5] 프로토콜을 이용하여 인증 정보의 보안성을 제공하고 있다. 그러나 이와 같은 보안 구조에서 문제점이 드러남에 따라서, IETF AAA WG에서는 유무선 통합망 환경에 적합한 새로운 형태의 AAA(인증/권한제어/과금) DIAMETER 프로토콜 규격을 표준화하고 있다. WEP 알고리듬에서는 키 스트림의 단순성으로 인한 실시간 공격과 도청으로 인한 평문의 노출, DoS 공격이 가능하다는 문제점이 있고[6], 클라이언트/서버 프로토콜인 RADIUS는 큰 규모의 적용환경에 취약한 것으로 알려져 있다[7].

(그림 1)의 WEP은 무선랜 데이터 스트림의 보안성을 제공하기 위하여 1997년 IEEE802.11 표준에 정의된 암호화 스킴으로서, 데이터의 암복호화에 동일키와 알고리듬을 사용하는 대칭형 구조이다. WEP 키는 단말을 인증하고, 데이터 프라이버시를 제공하는 데 사용된다. 액세스포인트의 서비스를 받는 모든 단말은 40비트 크기의 암호키를 공유하고 있다. 액세스포인트는 단말을 인증하기 위해 random challenge를 보내면, 단말은 40비트의 암호키와 24비트의 IV(Initialization Vector)를 결합하여 이를 RC4 암호화 알고리듬에 입력시켜 의사 난수 키 스트림을 생성하고, 이를 이용해 평문을 암호화



(그림 1) WEP 방식 암호화

하여 전송한다((그림 1) 참조). 액세스포인트는 이를 복호화하여 단말을 인증한다[3].

III. 새로운 무선랜 보안 구조

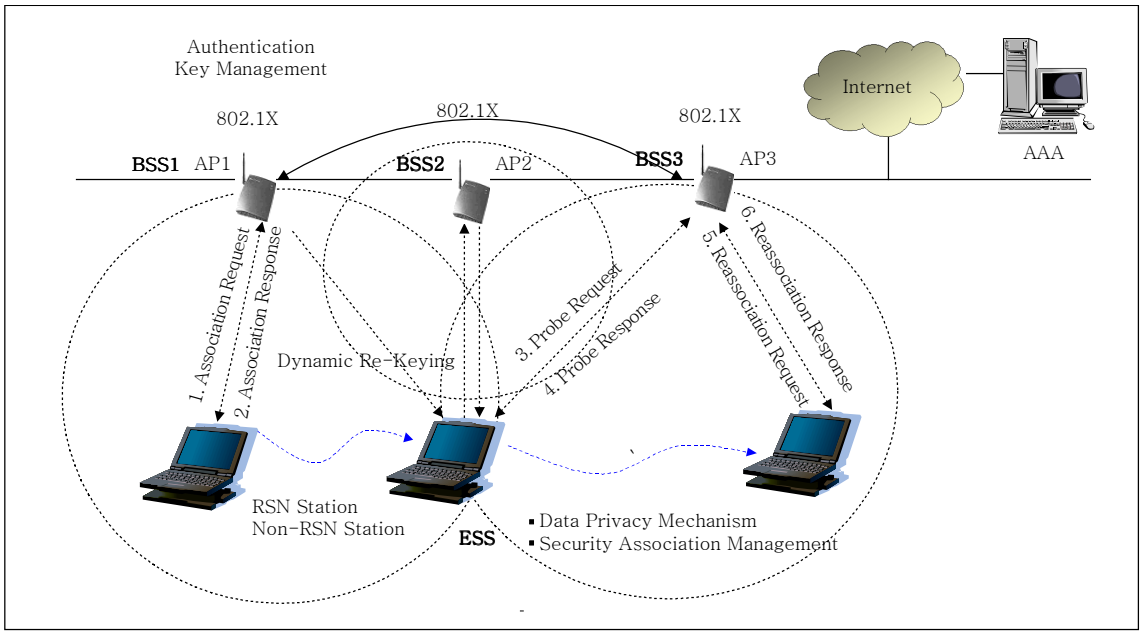
1. RSN

[1]은 WEP 방식의 보안 문제점이 WEP 키와 IV 사이즈가 작고, 모두에게 알려진 공유키를 사용하며, 암호 알고리듬(RC4)과 무결성 알고리듬(CRC-32)이 근본적으로 보안에 취약하다는 사실에 있음을 분석하였다. IEEE802.11i에서는 이러한 문제를 해결하는 방법으로 두 가지 접근 방식을 채택하고 있다. 하나는 장기적인 관점에서 알고리듬 자체를 보안 강도가 높은 알고리듬(AES-OCB)으로 바꾸는 것인데, 이러한 방식은 MAC 칩 하드웨어를 변경하여야 하므로 개발기간이 길고, 기존에 배치되어 사용중인 무선랜에 backward compatibility를 보장못하는 문제가 있다. 또 다른 하나는 단기적인 관점에서, 전술한 보안 문제점을 소프트웨어적으로 개선하는 TKIP(Temporary Key Integrity Protocol) 방식이다. 본 논문의 V장에서 TKIP이 어떻게 WEP 보안 문제점을 개선하는지 설명하겠다.

IEEE 802.11 WG는 무선랜 보안의 문제점을 다음과 같이 정리하고 표준화에 반영하고 있다. (1) RC4 WEP 알고리듬 자체가 알려진 평문 공격에 취약하다. (2) 동적인 WEP 키 분배 방법이 없다. (3) 가입자 인증 및 접속 제어 방법이 없다. (4) 공중망에 적용을 위한 중앙 집중형 인증/과금/권한제어(AAA) 방법이 없다. (5) 인증서, 보안토큰, ID/패스워드, SIM 등을 지원하는 다양한 가입자 인증 방식이 없다. (6) 로밍 보안을 지원하지 못한다. 전술한 문제점 중에서 (1)과 (2)는 802.11i WG에서 (3)은 802.1x에서 (4)는 IETF AAA WG에서 (5)는 IETF EAP WG에서 그리고 (6)은 802.11f[8]와 802.11i, IETF Seamoby와 Mobile-IP WG에서 표준화를 진행하고 있다.

IEEE 802.11i는 2002년 3월 RSN 보안 구조를 드래프트 표준에 반영함으로써, 무선랜에서의 데이터 프라이버시 기능을 더욱 강화하였다. RSN은 핫스팟에서 802.11과 802.11i를 지원하는 무선랜 액세스포인트들이 공존하는 환경에서, 802.1x를 이용한 가입자 인증 및 키관리 메커니즘과 빠르고 안전한 로밍 보안 프레임워크를 제시한 새로운 형태의 보안 구조이다((그림 2) 참조).

RSN이 지향하는 보안 목표는 첫째, 동적인 키갱신(dynamic rekeying) 등 무선 보안 강화(strong confidentiality) 기술을 이용한 보안의 취약성(기밀성, 무결성 등) 해결, 둘째, 다양한 무선망 환경, 즉 무선랜 인프라망과 Ad-Hoc 망에 유연하게 적용할 수 있는 보안(flexible security) 프레임워크 제시, 셋째, IEEE 802.1x를 적용한 가입자 상호 인증 및



(그림 2) RSN

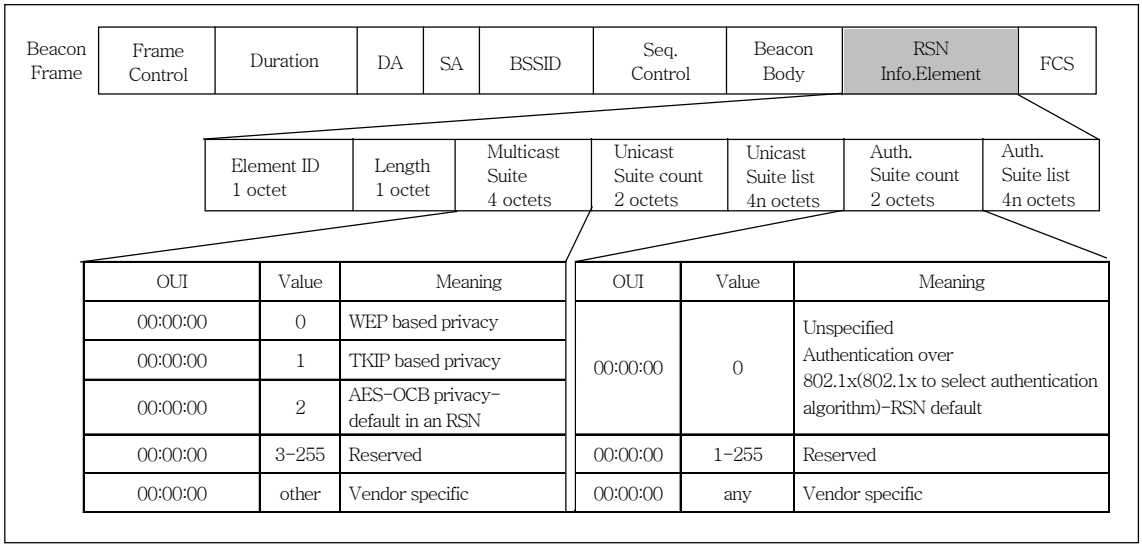
무선랜 망 접속제어(port-based network access control), 넷째, 액세스포인트와 인증서버를 분리함으로써 가입자의 제약 없는 글로벌 로밍 보안 지원(ubiquitous security), 다섯째, 액세스포인트를 이동하는 가입자와 신규 서비스를 요청하는 가입자 수에 확장성이 있으면서 빠르고 안전한 재인증 메커니즘을 제공하는 것이다.

RSN의 주요 보안 요소는 802.1x 인증 메커니즘, 802.11i 데이터 프라이버시 메커니즘, 그리고 보안 어소시에이션 관리이다. 802.1x 인증 메커니즘은 EAP/EAPOL 프로토콜, EAP 인증 및 키분배 알고리듬, AAA 인증서버, 그리고 논리적인 포트 기반 무선랜 접속 제어기술로 대변된다. 데이터 프라이버시 메커니즘은 WEP, TKIP, AES로 대변되는 세 가지 cipher suite로 구성된다. Cipher suite는 무선 데이터 프라이버시를 보장하는 데 필요한 인증 및 암호 알고리듬 세트를 의미한다. 보안 어소시에이션 관리는 동적인 키생성 및 분배 메커니즘과 re-keying 프로토콜을 이용하여 단말과 액세스포인트 간에 특정 cipher suite에 맞는 보안 컨텍스트를 설정하고 유지하는 과정이다.

2. RSN 보안 협상

RSN 보안 협상은 단말과 액세스포인트가 서로 간의 보안 요구사항(인증 메커니즘, 유니캐스트/멀티캐스트 암호알고리듬과 같은 cipher suite)을 일치시키는 절차로써, RSN 보안 프레임워크를 지원하기 위하여 2002년 3월 IEEE 802.11i 규격에 새로이 추가된 부분이다. RSN 보안 협상은 액세스포인트와 단말이 무선랜의 MAC association 설정 과정에서 진행된다. 협상에 필요한 cipher suite 파라미터들은 (그림 3)에서 보는 바와 같이 RSNIE(RSN Information Element) 구조체로 표현되며, MAC management 프레임(beacon, association, reassociation, probe 프레임)에 포함되어 단말과 액세스포인트 사이에 전달된다.

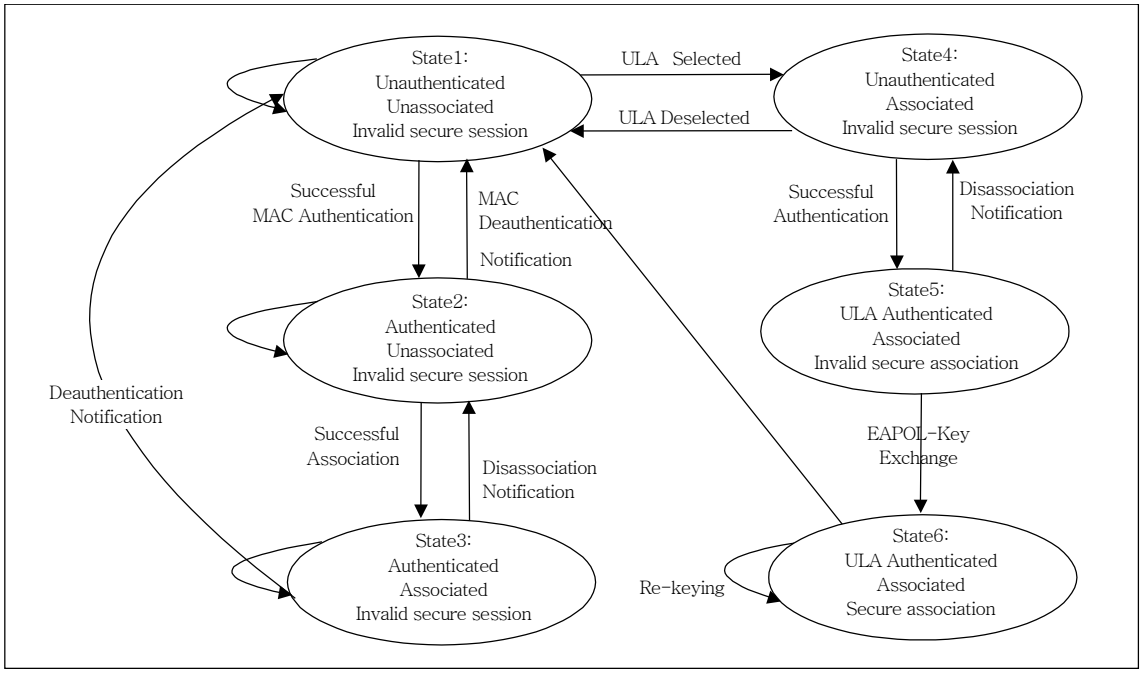
협상 절차는 다음과 같다. RSN을 인지하는 단말이 RSNIE를 포함하는 비컨 프레임을 받으면, 단말이 보안 어소시에이션 맺기를 희망하는 cipher suite의 값을 선택한다. 단말이 선택한 cipher suite는 (예를 들면 유니캐스트 알고리듬: TKIP, 멀티캐스트 알고리듬: AES, 인증방법: 802.1x) associa-



OUI	Value	Meaning
00:00:00	0	WEP based privacy
00:00:00	1	TKIP based privacy
00:00:00	2	AES-OCB privacy-default in an RSN
00:00:00	3-255	Reserved
00:00:00	other	Vendor specific

OUI	Value	Meaning
00:00:00	0	Unspecified Authentication over 802.1x(802.1x to select authentication algorithm)-RSN default
00:00:00	1-255	Reserved
00:00:00	any	Vendor specific

(그림 3) RSN 비컨 프레임 구조

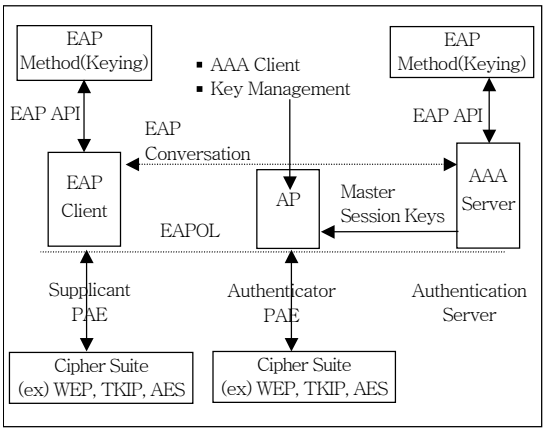


(그림 4) RSN 서비스 다이어그램

tion request 프레임에 실려서 액세스포인트로 전달된다. 액세스포인트는 단말이 요구한 cipher suite에 대한 협상 결과를 associate response 프레임을 통하여 알림으로써 단말과 액세스포인트 간의 보안 세션 설정을 개시한다. RSN 협상시 단말이 특별히 원하는 cipher suite를 제시하지 않으면 액세스포인트는 단말이 802.1x 인증 방식과 AES cipher suite에 의한 데이터 프라이버시 보장을 요구한다고 가정하고 보안 세션 설정을 시작한다.

일단 RSN 보안 협상이 완료되면 단말은 협상된

인증 방식에 따라서 인증을 수행한다. 인증이 완료된 후에, 단말과 액세스포인트는 선택된 암호 알고리듬(WEP, TKIP, AES)을 동작시키는 데 필요한 세부 키를 생성하고, 키교환 프로토콜을 이용하여 상호간의 키를 일치시킴으로써 보안 어소시에이션을 설정한다. 이렇게 형성된 보안 어소시에이션과 cipher suite들은 단말이 액세스포인트 사이를 이동할 때 반드시 전달되어야 하는 기본적인 보안 컨텍스트가 된다. (그림 4)는 기존의 MAC 서비스에 RSN 보안 서비스를 제공할 수 있도록 확장해 본 상태 천이도이다.



(그림 5) 802.1x 포트 기반 무선랜 접속 제어

IV. 802.1x 기반 인증 및 키 분배

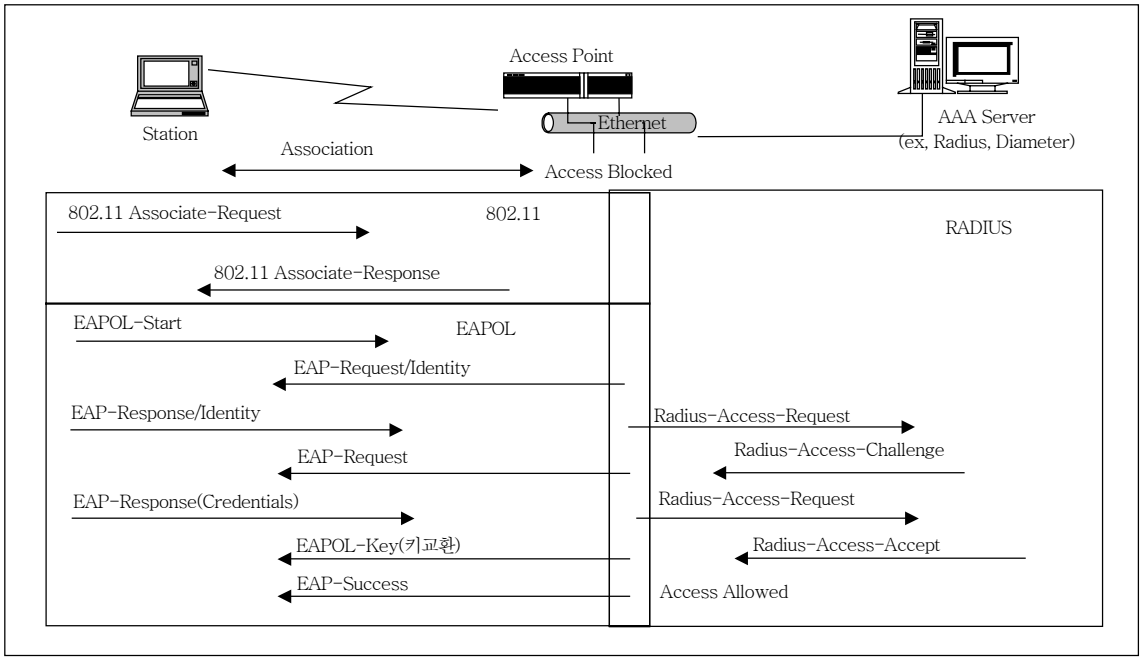
IEEE 802.1x는 무선랜 가입자의 상호인증 방법과 무선 접속구간 보안에 필요한 마스터 세션 키를 동적으로 분배하기 위한 방법을 정의한 규격이다. MAC 상위 계층에서 인증을 수행하여 합법적인 가입자에게만 무선랜 접속을 허용하기 위한 액세스 컨트롤 표준 규격을 제공한다. 가입자와 인증서버가 인증과정에서 동적으로 생성한 마스터 세션키를 인증서버로부터 액세스포인트로 키를 분배하는 역할을 수행한다((그림 5) 참조). 이렇게 분배된 키는 나중에 패킷 단위로 무선 접속구간의 데이터 프라이버시를 제공하기 위한 기본 키로 활용된다. 따라서 802.1x는 인증 주체(인증서버)와 액세스 컨트롤 주체(액세스포인트)를 이원화시킨 구조를 갖는다. 당연히 이러한 분리된 구조는 가입자의 글로벌 로밍을 용이하게 지원할 수 있는 장점이 있다.

(그림 5)에서 supplicant는 망접속을 요청하는 단말이고, authenticator는 단말과 인증서버 간의 인증과정을 중계하고, 인증 결과에 따라 액세스 컨트롤을 수행하는 주체(Port Access Entity: PAE)가 된다. 액세스 컨트롤 주체인 액세스포인트는 어소시에이션 ID와 같은 논리적인 포트를 이용하여 가입자의 접속을 제어한다. 즉 패킷 필터링을 통하여 인증받은 포트로 송수신되는 데이터만 전송을 허용하는 방식이다.

802.1x에서는 EAP(Extened Authentication Protocol)[9]를 가입자 인증 데이터 전송을 위한 표준 프로토콜로 이용하고 있다. 2002년 3월 현재 IETF에 EAP 워킹그룹이 설치되어 ID/패스워드, 인증서, 스마트카드 등 다양한 인증 방식을 지원하는 알고리듬과 각 인증 알고리듬을 이용한 세션 키 생성 방법의 표준화를 추진하고 있다.

1. 802.1x 프로토콜 동작

802.1x 프로토콜 동작은 비교적 간단하다. 사용자(supplicant PAE)가 먼저 접속을 시도하는 경우, EAP-start 메시지를 액세스포인트(authenticator PAE)에게 보낸다. 액세스포인트는 EAP-start 메시지를 받으면 가입자 인증에 필요한 가입자 신원(ID) 정보를 단말에게 요청한다. 이 때 가입자의 글로벌 로밍과 과금을 지원하기 위해서는 가입자 ID가 이메일 주소 표기와 같은 NAI(Network Access ID) 형식(예, cbh@etri.re.kr)을 따라야 한다[5]. NAI 형식을 준수해야 만이 가입자의 홈 인증서버의 위치를 알 수 있어서 분산 인증이 가능하게 된다. 이와 관련된 규격은 IETF[10],[11]에서 표준화를 진행하고 있다. 사용자로부터 받은 가입자 신원 정보는 AAA EAP-attribute 메시지[12]에 담겨져서 인증서버에게 전달되고, 최종적으로 액세스포인트는 인증서버로부터 인증 성공/실패 메시지 ((그림 6)의 Radius-



(그림 6) 802.1x를 이용한 무선랜 접속 과정

Access-Accept)를 받으면 인증과정이 종료된다. 이 때 인증과정에서 생성한 마스터 세션키는 Radius-Access-Accept 메시지에 담겨져서 액세스 포인트로 전달된다[13]. 그 다음에, 액세스포인트는 EAPOL-Key 메시지를 이용하여 단말과 키교환을 수행함으로써 키 사용 시점을 동기화한다. 그 후, EAP-success 메시지를 동기된 키로 암호화하여 보냄으로써 802.1x를 이용한 무선랜 접속이 허용되었음을 단말에게 알린다. 이 후부터 단말과 액세스 포인트는 동적으로 분배된 키를 이용하여 무선 데이터 구간에 대한 프라이버시를 보장받게 된다.

2. EAP 인증 유형

IETF EAP WG에서 표준화중인 EAP 인증 유형(EAP-method)을 <표 1>에 정리하였다[14]. EAP-MD5[15]는 EAP-method 중에서 유일하게 mandatory로 정의된 인증 방식이다. 구현이 단순하나 단방향으로 가입자 인증만을 지원하고, 무선랜 접속구간 보안에 필요한 마스터키 생성 방식을 정의하고 있지 않는다는 문제가 있다. EAP-TLS(Transport Layer Security)[16]는 사용자와 인증서버가 인증서를 이용하여 상호인증하고, 세션 기반의 동적인 WEP 키를 생성하여 분배하는 대표적인 인증 방식이다.

EAP-TTLS(Tunneled TLS Authentication Protocol)[17]는 EAP-TLS의 확장 형태이다. 열악한 무선 환경에서 무거운 인증서를 보관하고 전송하는 문제를 보완하기 위하여 단말 인증은 비밀번호로

<표 1> EAP 인증 방식 비교

EAP Method	Authentication Credentials	Authentication Server	Comment
EAP-TLS	Digital Certificates	Certificates Infastructure Required	Generate Keys
EAP-TTLS	Client-Password Server-Certificate	ServerCertificates Standard PAP, CHAP MSCHAP User Database	Generate Keys
EAP-SRP	Password only	Only Password Verifier Is Stored	Generate Keys
EAP-MD5	Password only	Standard MD5	Oneway Authentication No Key Generation

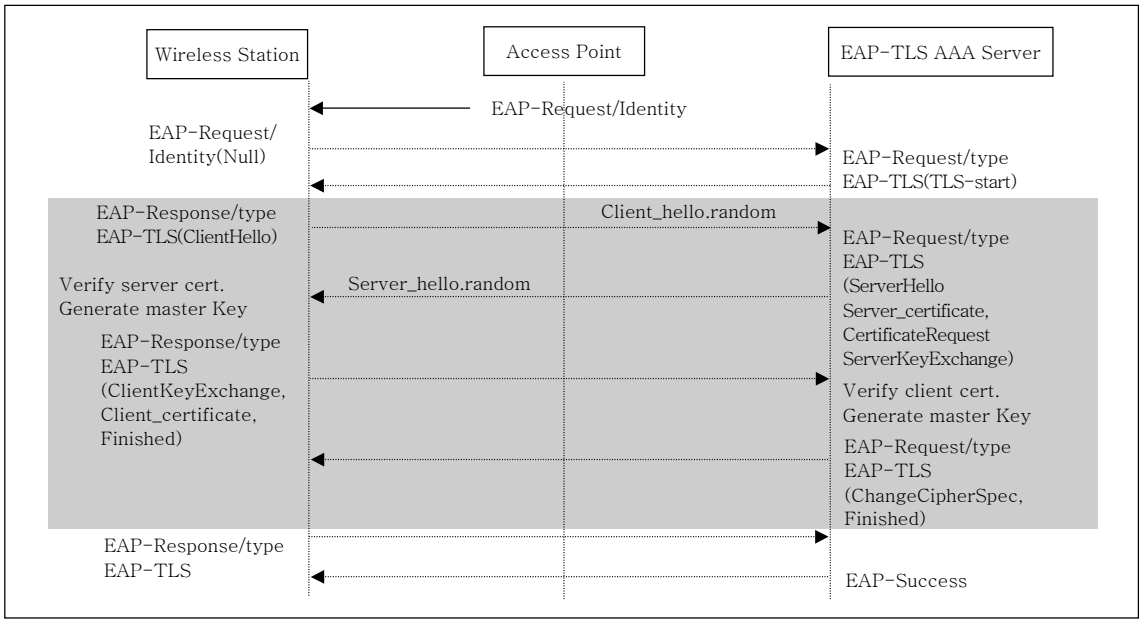
그리고 서버 인증은 인증서를 이용하여 인증하는 방식이다. 사용자 정보는 TLS 프로토콜을 통해서 안전하게 터널링 함으로써 무선링크를 포함한 인증서버까지 외부 도청자에 대한 익명성이 보장된다. EAP-AKA(Authentication and Key Agreement)[18]는 3GPP(3rd Generation Partnership Project)에서 IMT-2000용으로 제안한 인증 및 키 일치(AKA) 메커니즘을 EAP에 적용한 인증 방식이다.

3. EAP 마스터키 생성

EAP keying의 목적은 가입자와 인증서버가 EAP-method를 이용한 상호인증 과정에서 유도된 마스터키로부터 마스터 세션키를 생성(EAP keying)하는 것이다. 마스터 세션키는 인증서버에서 생성되고, 액세스포인트로 전달되어 무선 접속구간의 프라이버시를 보장하기 위하여 사용되는 키이다. 액세스포인트는 마스터 세션키로부터 초기 RSN 협상 과정에서 결정한 cipher suite의 크립토 키(Transient Session Key: TSK)를 생성한다. 이때 EAP-keying의 문제는 어떤 알고리듬을 이용하여 마스터키로부터 마스터 세션키를 유도할 것인가, 단일 유도 알고리듬을 제정하여 모든 EAP-method에 공통적으로 적용할 것인가, 그리고 이렇게 유도된 마스터 세션키를 어떻게 액세스포인트로 전달할 것인가 이다. IETF AAA WG와 EAP WG에서 이와 관련한 표준을 다루고 있으나 아직 국제 규격은 없는 상태이다. 마스터키를 유도하는 EAP-keying 알고리듬의 대표적인 EAP-TLS 프로토콜을 이용하여 전술한 EAP-keying 문제를 살펴보겠다.

(그림 7)은 인증서를 이용하여 단말과 인증서버가 상호 인증한 후 마스터 세션키를 생성하는 절차를 보인 그림이다. TLS(Transport Layer Security)는 인터넷 전송계층에 암호채널을 형성할 당사자들이 핸드셰이킹을 통하여 상호인증 및 키분배를 수행한 후, 송수신되는 모든 메시지를 대상으로 기밀성 서비스를 제공하는 보안 프로토콜이다. EAP-TLS는 TLS의 핸드쉐이크 메커니즘을 이용하여 무선랜 단말기와 인증서버를 상호인증하고, 양단 간에 마스터 세션키를 일치시키는 프로토콜이다.

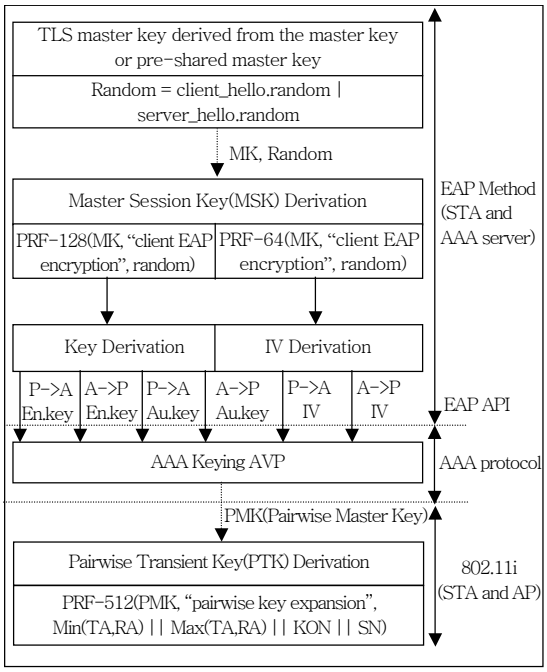
무선 단말이 802.1x를 이용하여 인증하겠다고 무선랜 접속을 시도하면, EAP-TLS(TLS-start) 메시지를 통하여 (그림 7)과 같이 핸드쉐이크가 시작된다.



(그림 7) EAP-TLS 상호 인증 및 키 분배

무선 단말은 핸드쉐이킹 과정에서 생성된 난수를 ClientHello 메시지에 포함시켜 서버로 전송한다. 인증서버도 난수를 포함한 ServerHello와 서버의 인증서, 그리고 단말의 인증서 요청 메시지를 보낸다. 무선 단말은 자신이 생성한 난수와 서버가 보내준 난수를 이용하여 공유키(pre-master key)와 마스터 세션키를 생성한 후, 서버의 공개키로 공유키를 암호화하여 서버에게 전송(ClientKeyExchange 메시지)한다. 이 때 마스터 세션키를 유도하는 함수는 (1)과 같다[19].

label = “client EAP encryption”;
PRF-128(pre-master key, label, nonce) =P_MD5(S1, label + nonce XOR P_SHA-1(S2, label + nonce);) ---- (1)
(S1 is first half of secret, S2 is second half of secret)



(그림 8) EAP-TLS 키 생성 및 분배

클라이언트로부터 ClientKeyExchange 메시지를 받은 서버는 자신이 가지고 있는 비밀키를 이용하여 공유키를 추출하고, 공유키와 2개의 난수(client_hello.random, server_hello.random)를 이용하여 마스터 세션 키를 생성한다. 상기 과정을 통하여 무선 단말은 서버를 상호 인증하고, 암호화를 위한 마스터 세션 키(128비트 암호키와 64비트 IV값)를 유도하게 된다((그림 8) 참조). 이렇게 유도된 마스터 세션키는 인증서버(예, RADIUS 또는 DIAMETER)의 AAA 프로토콜 메시지[12]에 실려서 액세스포인트에 전달된다. 전달된 키는 무선 데이터 프라이버시 보장을 위한 마스터키(Pairwise Master Key: PMK)로 불리우며, 이 PMK는 cipher suite를 실행하는 데 필요한 키(Pairwise Transient Key: PTK) 크기로 확대 생성한 후 세부 사용 목적에 따른 크기로 절단해서 사용된다.

이렇게 계층적으로 키를 생성하는 이유는 다음과 같다. 무선랜 보안에 사용될 키는 상호 인증된 키이어야 한다. 따라서 EAP-methods 수준에서 키가 생성될 수 밖에 없다. 그러나 문제는 EAP-method는 가입자와 인증서버 양단에서 동작하므로 무선단말과 액세스포인트가 RSN 협상 과정에서 어떤 cipher suite를 사용하기로 결정했는지, 즉 키 생성과 관련된 구체적인 키 요구사항을 상위 계층에서는 알 수 없다는 점이다. 결국 인증된 마스터 키는 EAP 수준에서 생성해서 액세스포인터로 보내고 실제 cipher suite에 필요한 키는 보안 어소시에이션 과정을 통하여 생성된 후 분배되어야 하므로 계층적인 키관리가 필요하다.

V. TKIP 보안 어소시에이션

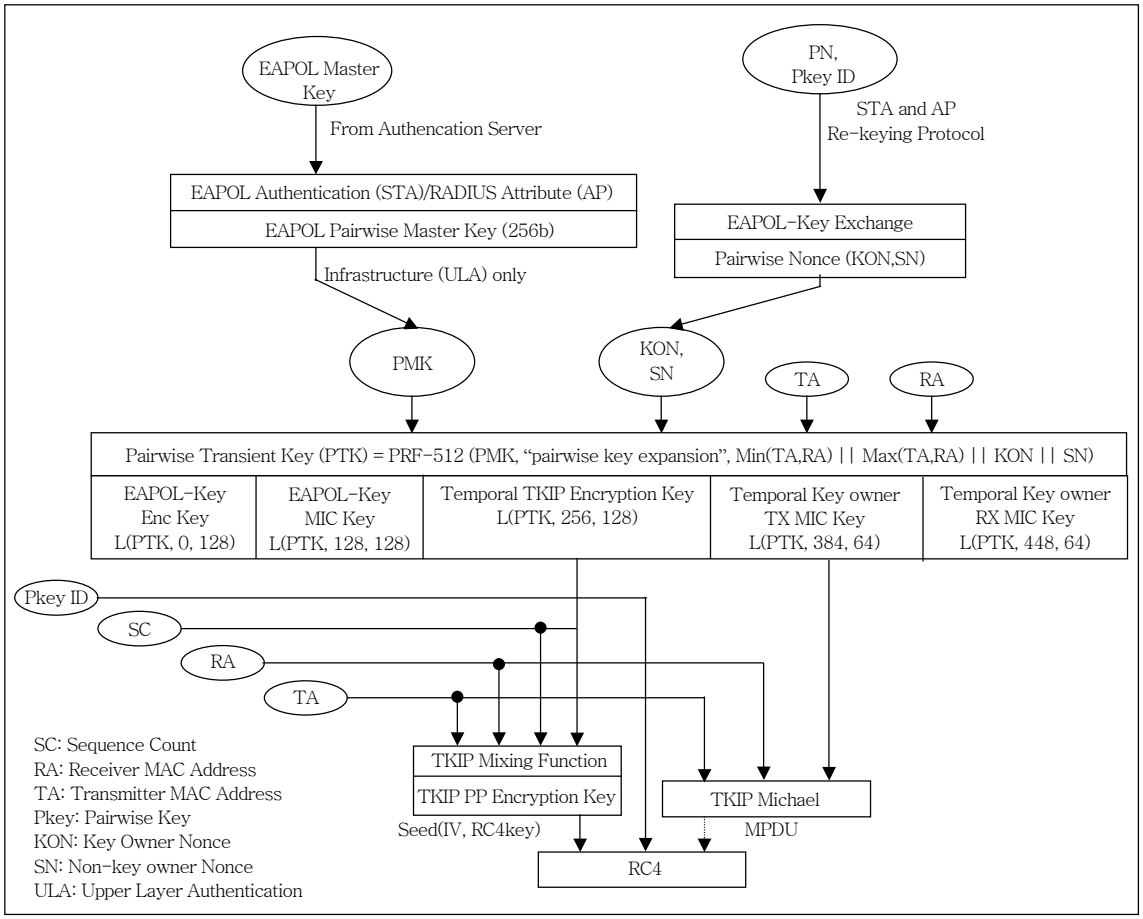
본 논문의 I장에서 언급하였듯이 WEP을 이용한 802.11b 무선랜 보안의 문제점은 첫째, 동적인 키 분배 방법이 없다, 둘째, 크기가 작은 IV값을 재사용한다, 셋째, per-packet 키가 없다, 넷째, 취약한 무결성 알고리듬을 이용한다는 점으로 요약할 수 있다. TKIP은 기존의 WEP RC4 보안의 문제점을 소프트웨어적으로 개선하여 단말과 액세스포인트에 패치하여 사용할 수 있도록 함으로써 이미 배치되어 사

용중인 무선랜의 보안 문제점을 해결하자는 취지에서 개발된 보안 프로토콜이다. TKIP 프로토콜은 key-mixing 함수, Michale MIC 함수, 키교환 프로토콜, re-keying 프로토콜로 구성된다((그림 10) 참조). 본 장에서는 TKIP을 이용해서 어떻게 보안 어소시에이션을 형성하고 관리하는지를 각 컴포넌트를 중심으로 설명하겠다.

1. TKIP 키의 계층성(Key Hierarchy)

(그림 9)는 TKIP 키의 계층적 구성도이다. 그림에서 PMK는 앞서 설명한 바와 같이 EAP 인증 후에 AAA 서버에서 액세스포인트로 전달된 키이다. 액세스포인트에는 키 매니저가 있어서 무선 단말과 키교환 프로토콜을 수행하여 무선 구간 보안 서비스에 필요한 세부 기능키를 생성하고, 키의 사용 시점 즉 보안 세션을 동기화 시킨다.

(그림 9)에서 TKIP용 PTK 키는 512비트로 구성되며, 512비트는 4개의 128비트(EAPOL Encryption 키, EAPOL MIC 키, 그리고 TKIP Encryption 키)와 2개의 64비트(TKIP Tx MIC 키, TKIP Rx MIC 키)로 분해되어 EAPOL 키 교환 과정에서의 기밀성과 무결성, 그리고 데이터 패킷 송수신 과정에서의 기밀성과 무결성 서비스 보장에 활용된다. PTK 키 유도 알고리듬은 아직 표준안으로 채택되지는 않았지만 EAP-keying에 이용된 (1)의 PRF 알고리듬을 이용하는 방향으로 논의되고 있다.



(그림 9) RSN TKIP Pairwise 키 계층도

PTK = PRF-512(PMK, “pairwise key expansion”, Min(TA,RA) ||Max(TA,RA) || KON || SN) --- (2)
(TA: 단말의 MAC 주소, RA: 액세스포인트의 MAC 주소, KON: 액세스포인트가 생성한 난수, SN: 단말이 생성한 난수)

(2)의 PTK 유도알고리듬은 가입자와 인증서버 간의 상호인증 결과로 생성된 PMK, 단말기와 액세스포인트의 MAC 주소, 그리고 단말기와 액세스포인트가 EAPOL 키교환 과정에서 서로 주고 받은 난수를 결합하여 키가 생성됨을 알 수 있다.

2. Key Mixing과 Michael 함수

(그림 10)은 TKIP의 암호화 과정을 보인 블록도이다. Key-mixing 함수는 가입자의 per-packet 키를 생성하는 함수이다. 키생성 절차는 2단계로 이루어진다.

TTAK ← Phase1(TKIP Enckey, TA)
WEP seed ← Phase2(TTAK, SeqCounter)

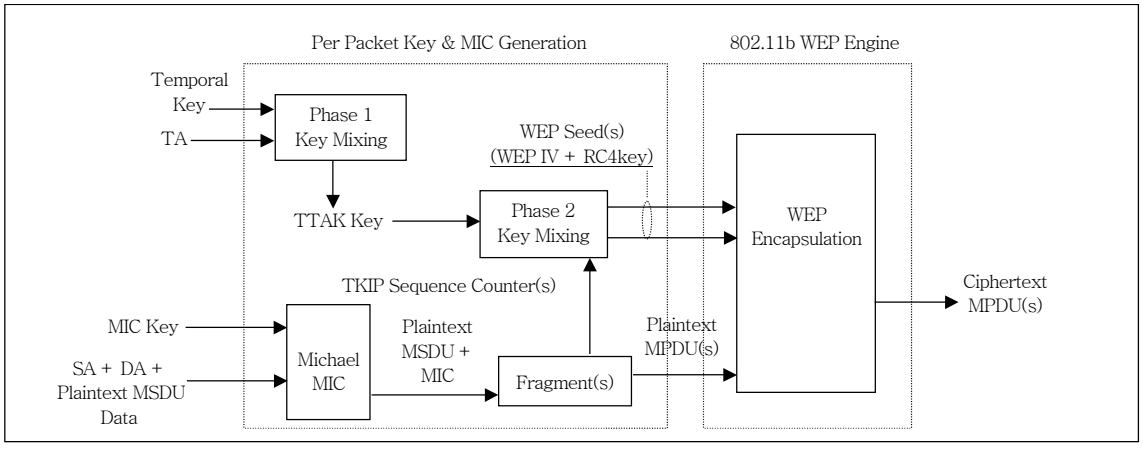
1단계에서는 TKIP Encryption key와 단말(transmitter)의 MAC 주소를 이용하여 Temporary TA key(TTAK)를 생성하고, 2단계에서는 128비트 TTAK와 16비트 sequence counter를 이용하여 128비트 WEP seed를 생성한다. 이렇게 생성된 키는 802.11b의 WEP 암호화를 위한 105비트 RC4키와 24비트 WEP IV로 활용된다.

Michael 함수는 기존의 WEP 방식에서 CRC-32를 이용한 메시지 인증방식의 문제점을 개선하기 위하여 새롭게 제안한 메시지 인증 함수로서 64비트 TKIP MIC 키, 소스/목적지 MAC 주소와 MSDU 메시지를 결합하여 인증 코드를 생성한다. 이렇게 생성된 코드는 key-mixing 함수에 의해서 생성된 WEP seed로 암호화하여 전송된다.

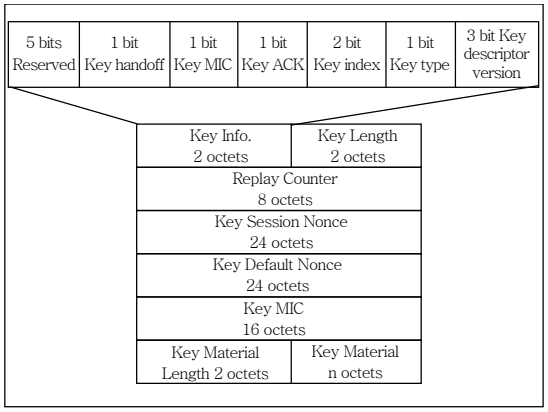
3. 키교환 및 동기화(Automatic Key Exchange and Synchronization)

802.1x에 의해서 가입자 인증이 완료되면, 인증서버는 Radius-Access-Accept 메시지에 PMK를 실어서 액세스포인트에게 전달한다((그림 8) 참조).

액세스포인트에 위치한 인증 클라이언트는 전달받은 Radius-Access-Accept 메시지를 해석한 후 PMK를 키 메니저에게 전달함으로써 단말기와 액세스포인트 간의 키교환이 수행된다. 이렇게 함으로써 무선단말기, 액세스포인트, 인증서버 모두가 동일한 PMK를 보유할 수 있게 된다. 무선 구간에서 키교환을 위한 프로토콜은 (그림 11)과 같은 EAPOL(EAP over LAN) key descriptor를 이용하여 진행된다.



(그림 10) TKIP 암호화 과정



(그림 11) EAPOL-Key Descriptor

Key descriptor는 키교환이 이루어지는 시점(핸드오프 또는 초기 접속과정), 교환할 키 유형이 group 키인지 pairwise 키인지 여부, 그리고 단말과 액세스포인트 간의 PTK 생성에 필요한 난수, 메시지 인증을 위한 MIC 코드, 그리고 replay attack 방지를 위한 sequence count에 대한 정보를 포함한다.

EAPOL Key Descriptor를 이용한 키 교환 절차는 (그림 12)와 같다. 그림에서 보여주는 키교환 절차는 세 가지의 의미를 갖는다. 첫째, 키생성에 필요한 난수를 교환함으로써 키생성과 동시에 보안 어소시에이션을 맺는 것이고, 두번째는 암복호화에 사용될 세 개의 키(두 개의 pairwise Ping/Pong key, 1개의 group)를 생성하는 것이다. 두 개의 pairwise 키 중 하나는 암호화용 키로서 그리고 나머지 하나는 IV 사용 한도에 도달했을 때 대체를 위한 갱신용 키이다. 셋째, 802.1x 인증과정의 마지막 메시지인 EAPOL-success 메시지를 암호화해서 송신함으로써 키 사용 시점을 동기화하는 것이다.

4. 키 갱신 프로토콜(Re-keying Protocol)

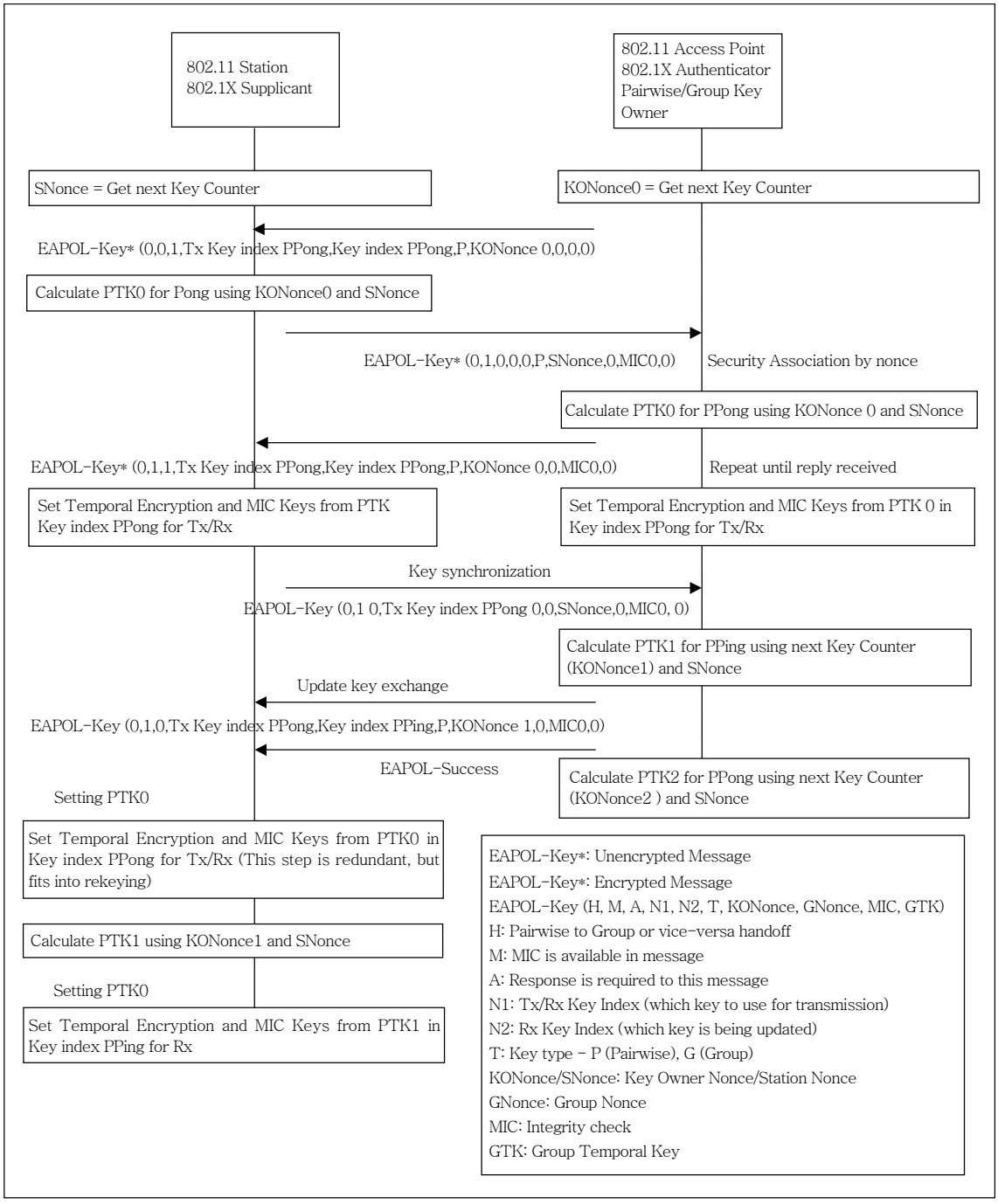
(그림 13)은 re-keying 절차이다. 사용중인 키의 sequence-count(IV)가 한도에 도달할 경우 보안강도를 유지하기 위해서 사용중인 PTK를 갱신하는 절차이다. Re-keying은 일관성 보장을 위하여 암호화된 모든 수신 메시지들의 복호화가 완료된 후에 시작된다. 키 갱신을 위해서는 먼저, 초기 키교환 과정((그림 12) 참조)에서 설정해 놓은 2개의 pairwise 키 중에서 대체용 키를 주 암호키로 설정한 후, 액세스포인트 주도로 키 생성에 필요한 난수를 단말과 교환한다. 교환된 난수를 이용하여 다음 갱신용 키와 다음 암호화 키를 생성한다. Re-keying 과정에서 이용되는 EAPOL-key 메시지는 EAPOL-key MIC 키를 이용하여 메시지 인증을 수행하고, EAPOL-key encryption 키를 이용하여 암호화하여 송수신함으로써 대체된 주 암호키의 사용 시점을 상호 동기화시킨다.

VI. 결론 및 향후 전망

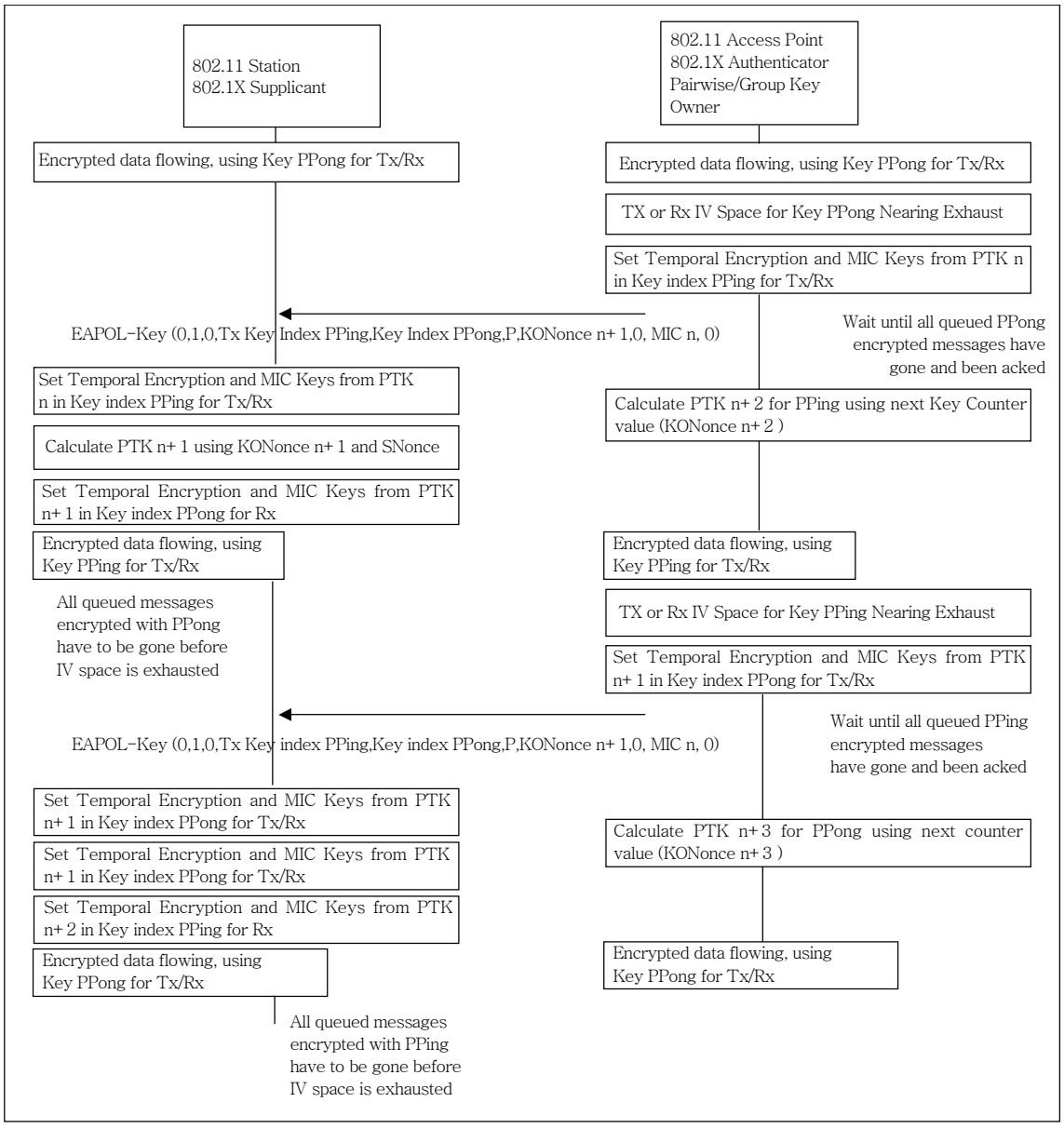
현재 무선인터넷 사업자(WISP)들은 핫스팟 지역에서 무선랜을 기반으로 하는 고정 무선인터넷 서비스를 시작하고 있다. 그러나 머지 않아 액세스포인트 공유를 통하여 무선인터넷 사업자 간의 무선랜 글로벌 로밍 서비스와 함께 Mobile-IP 기반의 이동 인터넷 서비스가 예상된다.

IETF Mobile-IP 워킹그룹에서는 무선랜에서 빠른 핸드오프 지원을 위한 기술 표준화 논의를 활발하게 진행하고 있고, IEEE 802.11i와 802,11f에서는 동일한 서브넷에 위치한 액세스포인트들 간의 이동시 제공해야 할 로밍 및 마이크로이동 보안에 대한 표준화 논의(authenticated fast 핸드오프 지원, 핸드오버 과정에서 보안 어소시에이션 유지, 로밍 매니저 등)를 진행하고 있다. 무선랜에서 글로벌 로밍 서비스가 제공되기 위해서는 분산인증 및 실시간 패킷과금에 대한 요구 또한 더욱 중요시된다. 이와 관련하여 이동통신과 무선랜이 연동되는 이동 인터넷 환경에 적합한 DIAMETER AAA 서버의 표준화를 IETF AAA 워킹그룹에서 진행하고 있다. 무선랜 보안과 관련한 또 하나의 중요한 기술은 무선랜 Ad-Hoc 망에 대한 보안이다. Ad-Hoc 망은 IEEE 802.15의 WPAN과 함께 4세대 이동통신 액세스 네트워크의 중요한 기술로서 인식되고 있다. 본 논

문은 무선 고정인터넷 서비스 제공에 필요한 무선랜 가입자의 인증 및 키관리 기술을 중심으로 표준화 동향을 기술하였다. 본 논문에서는 기술하지 않은 무선랜 로밍 및 이동보안, DIAMETER AAA 보안, 그리고 무선랜 Ad-Hoc 보안 이슈에 대한 지속적인 연구가 필요하다고 판단된다.



(그림 12) TKIP Pairwise 키 교환 초기화 과정



(그림 13) Pairwise 키 갱신 절차

참 고 문 헌

[1] J. Walker, "Unsafe at Any Key Size: an Analysis of the WEP Encapsulation," *Tech. Rep. 03628E, IEEE 802.11 committee,* March 2000, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.

[2] IEEE Std 802.11i/D2.0, "Specification for Enhanced Security," Mar. 2002.

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

[4] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June 2000.

[5] C. Finscth, "An Access Control Protocol, Sometimes Called TACACS," IETF RFC 1492, July 1993.

[6] W.A. Arbaugh, "Your 802.11 Wireless Network has No Clothes," University of Maryland, Mar. 2001.

[7] "http://www.interlinknetworks.com/references/Introduction_to_Diameter.html," Feb. 2002.

[8] IEEE Std 802.11f/D3, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," Jan. 2002.

[9] L. Blunk *et al.*, "PPP Extensible Authentication Protocol(EAP)," IETF RFC 2284, Mar. 1998.

[10] B. Aboba and M. Beadles, "The Network Access Identifier," IETF RFC 2486, Jan. 1999.

[11] P. Calhoun and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4," IETF RFC 2794, Mar. 2000.

[12] P. Calhoun, Allan C. Rubens, J. Haag, G. Zorn, "Diameter NASREQ Application," draft-ietf-aaa-diameter-nasreq-09.txt, IETF work in progress, Mar. 2002.

[13] D. Simon *et al.*, "RADIUS Master Session Key Attribute," http://www.potaroo.net/ietf/ids/draft-simon-radius-key-attr-00.txt, Mar. 2000.

[14] D. Stanley, "Advances in Security for Wireless lans: Authentication & Encryption," *IEEE Wireless lans and Home Networks conference*, Dec. 2001.

[15] D. Potter *et al.*, "PPP EAP MS-CHAP-V2 Authentication Protocol," http://www.rfc-editor.org/internet-drafts/draft-dpotter-pppext-eap-mschap-01.txt, Jan. 2002.

[16] P. Funk *et al.*, "EAP Tunneled TLS Authentication Protocol," http://www.potaroo.net/ietf/ids/draft-ietf-pppext-eap-ttls-01.txt, Feb. 2002.

[17] P. Calhoun and C. Perkins, "PPP EAP TLS Authentication Protocol," IETF RFC 2794, Mar. 2000.

[18] J. Arkko *et al.*, "EAP AKA Authentication," http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-03.txt, Feb. 2002.

[19] T. Dierks *et al.*, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan. 1999.