특

무선 LAN 환경에서 요구되는 보안 기술

송 지 은[1] 왕 기 철[2] 김 태 연[3] 조 기 환[4]

목 차

1. 서 론

이동 통신 서비스의 급속한 확장과 데이터 서비스에 있어서 이동성과 편리함을 추구고자 하는 소비자들의 욕구에 힘입어 무선 LAN은 기존 유선 LAN과 3G 무선 데이터 서비스의 단점을 일부분 보완할 수 있는 저렴하고 효과적인 무선 데이터 통신 솔루션으로 기대를 모으고 있다. 국내에서도 KT, 하나로통신, 데이콤, SK텔레콤 등 여러 통신 서비스 사업자들이 앞다투어 공중 무선 LAN 서비스(Public Wireless LAN Service)를 전개해 나가고 있어 무선 LAN에 대한 일반 인지도가 향상되었고 늦어도 올해 안에 54Mbps급의 무선 LAN 표준이 확정될 예정이어서 무선LAN이 제2의 성장기를 맞게 될 것으로 예측된다[1].

그러나 무선 LAN 사용이 늘어난 반면 안전한 무선 LAN 사용을 보장할 만한 무선 LAN 보안 솔루션은 상대적으로 취약한 편이다. 무선 LAN을 이용한 망은 브로드캐스트 망이라는 특성상 도청(eavesdropping)이 쉽고, 무선 장비의 노출로 해킹이 용이하다. IEEE 802.11b 표준에서는 WEP(Wired Equivalent Privacy) 프로토콜과 같은 무선 LAN 보안 방법을 제안하였으나 키 스트림의 단순성으로 인한 실시간 공격, 도청으로 인한 평문 노출과 DoS 공격의 가능성, 동적인 WEP 키 분배 방법의 부재 등의 보안상 취약점이 드러났다[2]. 이어서 802.11b의 한계를 보완하고 보안성을 강화시키기 위해 IEEE 802.1x가 제안되었다. IEEE 802.1x는 무선 LAN 가입자의 상호인증 방법과 무선 접속 구간 보안에 필요한 마스터 세션키를 동적으로 분배하기 위한 방법을 정의한 규격이다. 그러나 802.1x 역시 세션 하이제킹(Session Hijacking) 공격, 중간자 공격(Man-in-the-middle attack), 사전 공격(Dictionary attack) 등 해커의 공격을 받기 쉽다는 점이 지적되고 있다[3].

최근 IEEE 802.11i 워킹그룹은 보다 강력한 보안 서비스를 제공하기 위해 무선 LAN 인프라 망과 Ad hoc 망에 적용할 수 있는 RSN(Robust Security Network)이라는 새로운 형태의 보안 아키텍쳐를 제안하고 이에 대한 표준화를 진행하

1) 현재 전북대학교 컴퓨터정보학과(석사과정)
2) 전북대학교 컴퓨터 통계 정보학과 박사과정
3) 서남대학교 컴퓨터정보통신학과 조교수
4) 전북대학교 전자정보공학부 조교수

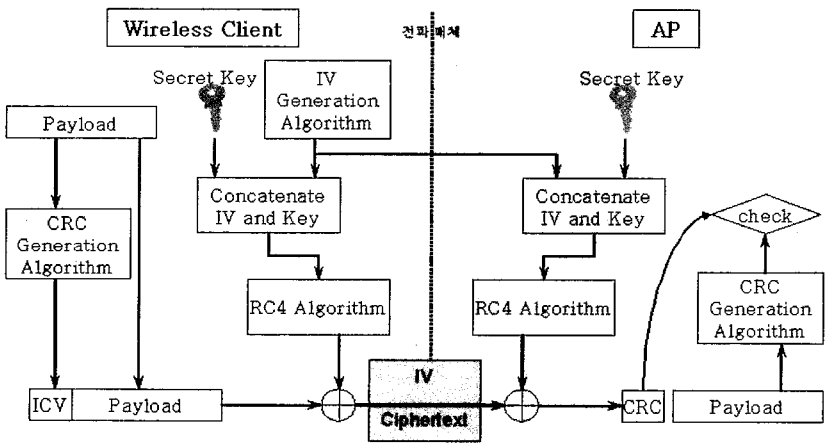
고 있다. RSN은 다수의 액세스 포인트가 연결된 핫스팟 지역에서 802.1x 기반 가입자 인증을 통한 액세스 제어, 보안 세션 관리, 새로운 알고리즘을 이용한 무선 구간 보안 강화 등을 지원함으로써 기존의 802.11 무선 LAN의 보안상의 취약점을 상당 부분 해결할 수 있을 것으로 기대된다.

본 고에서는 먼저 기존 무선 LAN망인 IEEE 802.11b의 보안상의 취약점에 대해 2장에서 정리한다. 이어 3장에서는 향상된 무선 보안 LAN 기술로 제안되고 있는 RSN의 표준화 동향과 Security Association, 802.1x 인증, Data Privacy와 같은 RSN 보안 요소에 대해 살펴본다. 또한 IEEE 802.15의 WPAN과 함께 4세대 이동 통신 액세스네트워크의 중요한 기술로써 인식되고 있는 무선 LAN Ad hoc망에서 고려되어야 할 보안상 이슈들에 대해 알아본다. 마지막으로 보다 안전한 무선 LAN 서비스를 위한 무선 LAN 보안 기술들에 대해 살펴보고 4장에서 결론을 맺는다.

2. 기존 무선 LAN 보안 기술의 취약점

IEEE802.11 에서는 유선 LAN과 비슷한 수준의 보안을 무선 LAN에 제공한다는 의미를 가진 WEP을 통해 인증 및 보안서비스를 제공한다. WEP은 데이터의 암·복호화에 동일키와 알고리즘을 사용하는 대칭형 구조이며 RC4 스트림 키 퍼를 암호화 알고리즘으로 사용한다. 또한 CRC-32를 이용해 데이터 무결성을 확인하며 24 비트의 IV(Initialization Vector)를 이용해 키 스트림을 생성하는 구성을 가진다. 그런데 이와 같은 WEP 프로토콜에 대해 많은 보안 결함들이 발견되었으며 크게 인증에 관한 문제와 WEP 알고리즘 자체에 관한 보안상 문제로 나누어 볼 수 있다[4].

먼저, WEP을 통해 인증 및 데이터를 암복호화하는 과정을 살펴보면 다음과 같다. (그림 1)과 같이 액세스 포인트가 단말을 인증하기 위해 random challenge를 보내면, 단말은 40 비트의 암호화키와 IV를 결합하여 RC4 암호화 알고리즘에 입력해 의사 난수 키 스트림을 생성한다. 또한 데이터로부터 CRC-32를 계산하여 ICV (Integrity Check Value)를 생성하고, 이 ICV와 데이터를 키 스트림과 XOR하여 평문을 암호화해 전송한다. 이를 수신한 액세스 포인트는 이를 복호화 하여 단말을 인증한다.



(그림 1) WEP 암/복호화 블록 다이어그램

그런데 이와 같은 WEP 방식의 인증은 모두에게 알려진 공유된 비밀키를 사용하여 비밀키의 유출이 쉽고 "challenge-response" 구조의 특성상 man-in-the-middle 공격에 취약하다. 또한 키 분배 방식이 정립되지 않아 대개의 경우 각 단말에 공유키를 손수 입력해야 하므로 키 관리가 어렵다. 또한 사용자 인증이 지원되지 않으므로 단말을 분실하거나 단말이 여러 사람에게 공유되어 사용되는 경우 엄격한 인증을 실행하기 어렵다는 취약점이 있다.

한편 WEP 알고리즘상 문제점으로는 다음과 같은 사항들이 있다. 키 길이가 80bit 이상이 되어야 Brute-force 공격이 불가능하다고 알려진 연구결과에 비해 대부분의 무선 LAN에서는 40bit의 WEP 키가 이용되고 있어 기밀성 보장에 위협을 받을 수 있으며 데이터의 무결성을 제공하기 위해 제공되는 ICV의 경우 ICV를 생성하는 CRC-32가 선형특성을 가지고 있어 공격자가 키를 알지 않고서도 전송중인 패킷을 변경하는 것이 가능하다. 또한 IV의 재사용을 허용함으로써 키 스트림 값의 유출로 암호화된 패킷의 해독이 가능하다는 문제점이 있다[5]. IEEE802.11i에서는 이러한 단점을 극복하기 위해 WEP2나 AES(Advanced Encryption Standard) 등의 보다 강력한 암호화 프로토콜을 제안하고 있다.

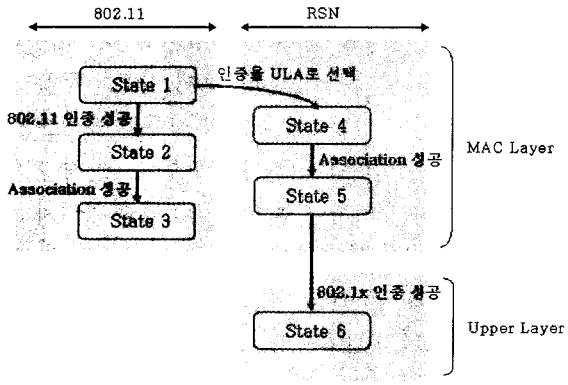
3. 향상된 무선 LAN 보안 기술

3.1 RSN(Robust Security Network)

IEEE 802.11 TGi는 기존의 802.11 무선 LAN에 QoS와 보안을 강화하기 위해 결성된 TGe에서 무선 LAN 보안 부분만을 따로 분리하여 2001년 구성되었다. IEEE 802.11 TGi에서는 장기적인 관점의 802.11 보안 아키텍처로 RSN을 제안하였다. RSN은 기존의 취약했던 인증 및 키 분배 문제를 해결하기 위해 IEEE 802.1x 프레임워크를 이용하여 동적인 키 생성 메커니즘의 부재를 해결하고 MAC 상위 계층의 사용자 인증 및 무선 LAN망 액세스 제어 등을 지원하도록 하고 있다. 802.1x의 사용은 액세스 포인트와 인증 서버를 이원화된 보안 구조 상 포인트 확장성과 유연성이 높아져 글로벌한 가입자 로밍 지원이 더욱 확대시킬 수 있는 이점도 있다. 또한 TKIP(Temporary Key Integrity Protocol)과 AES-OCB(AES-Offset Code Book)와 같은 더욱 강력한 암호화 프로토콜들을 제안하여 802.11 WEP의 데이터 프라이버시를 강화하였다.

RSN 보안은 기본적으로 보안 association 관리와 데이터 프라이버시 메커니즘이라는 두 가지 기본 서브시스템으로 구성된다. 보안 association 관리에 대해서는 다음과 같은 세 가지 컴포넌트를 정의하고 있다. 보안 Context를 구축하는 RSN 협상과정(negotiation procedure)과 EAP(Extend Authentication Protocol) 인증을 통해 허가된 사용자에게만 포트 기반 액세스 허가를 지원하는 IEEE802.1x 인증 메커니즘, 그리고 마지막으로 암호화키를 분배하기 위한 IEEE 802.1x 키 관리 메커니즘이 있다. 또한 데이터 프라이버시 메커니즘을 지원하기 위해 TKIP과 AES 기반의 두 가지 프로토콜을 정의하고 있다[5].

RSN의 대략적인 프로시저는 다음 (그림 2)와 같다. 인증을 ULA(Upper Layer Authentication)로 선택할 경우 공유키 인증 과정 없이 바로 이동단말과 AP(Access Point)간에 보안 세션을 구축하기 위해 RSN association 관리에 들어간다. 이어 RSN 보안 협상이 종료되면 협상 결과에 따른 사용자 인증 및 키 분배 과정이 진행되고 인증이 성공할 경우 단말과 AP 그리고 인증 서버간에 security association관계가 형성되어 State 6에서 사용자의 권한에 따른 통신이 이루어진다. 무선 구간상의 보안을 위해 기존의 WEP의 취약점



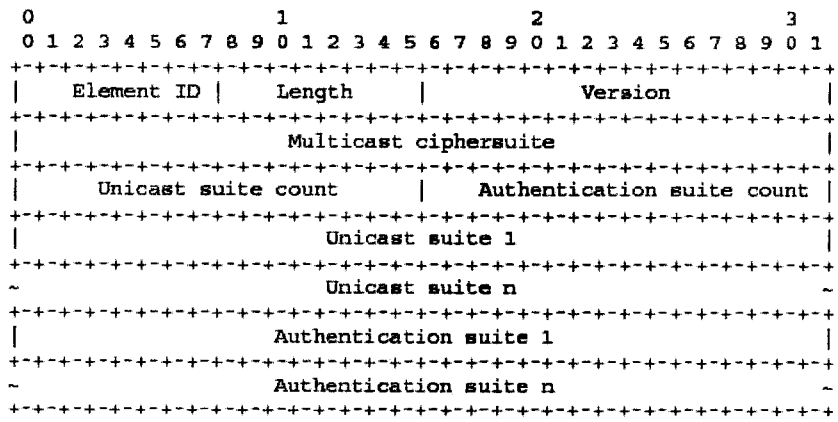
(그림 2) RSN 프로시저 상태도

을 개선하여 보다 강한 무선 구간의 데이터 프라이버시를 지원하기 위한 새로운 알고리즘이 사용된다.

3.2 RSN Security Association 관리

RSN 보안 협상 과정은 이동 단말(supplicant)과 AP(Access Point)간에 인증 메커니즘인 ASE(Authentication Suite Element)와 유니캐스트/멀티캐스트에 관한 협상인 UCSE (Unicast Cipher Suite Element)와 MCSE (Multicast Cipher suite Element). 그리고 NE(Nonce Element) 에 관한 보안 파라미터를 일치시키는 과정이다. ASE, UCSE, MCSE, NE와 같은 정보가 담긴 엘리먼트를 RESINE (RSN Information Element)라 하며 다음 (그림 3)과 같은 구조를 갖는다.

RSN 지원 가능한 AP는 RESINE 정보를 비콘 신호안에 포함하여 광고(advertisement)한다. 비콘 신호를 받은 이동 단말은 원하는 Cipher Suite Element(예: UCSE 알고리즘 - TKIP, MCSE 알고리즘 - AES, ASE: 802.1x)를 선택하여 Association Request 프레임에 포함시켜 AP에 전송한다. AP에서는 이동 단말이 요구한 Cipher Suite에 대한 협상 결과를 Association Response 프레임을 통해 응답함으로써 단말과 AP간의 보안 세션 설정을 시작한다. 그런데 RSN 협상 시 단말이 특별히 원하는 Cipher Suite를 제시하지 않으면 액세스 포인트는 단말이 802.1x 인증방식과 AES Cipher Suite를 요구한다고 가정하고 보안 세션 설정을 시작한다. 〈표 1〉은 각각 ASE와 CSE의 selector를 나타낸 프레임 구조다[5].



(그림 3) RSN Element Format

〈표 1〉 ASE와 CSE selector 프레임 구조

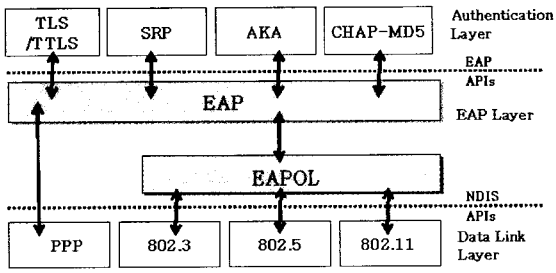
OUI	Type	Meaning
00:00:00	0	None
00:00:00	1	Unspecified authentication over 802.1x:default for RSN
00:00:00	2	Pre-Shared Key over 802.1x
00:00:00	3-255	Reserved
00:00:00	Any	Vendor Specific

OUI	Type	Meaning
00:00:00	0	None
00:00:00	1	WEP
00:00:00	2	TKIP
00:00:00	2	Reserved for AES cipher : Default for RSN
00:00:00	3-255	Reserved
00:00:00	Any	Vendor Specific

3.3 802.1X 인증 메커니즘 [5][6]

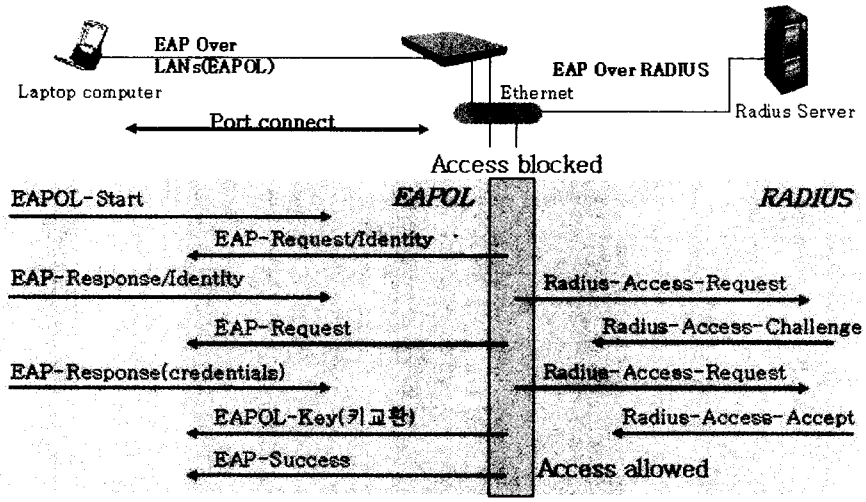
일단 RSN 보안 협상이 완료되면 단말은 협상된 인증 방식에 따라 인증을 수행한다. IEEE 802.1x는 ULA 프로토콜로서 세 가지 PAE (Port Access Entity)인 Supplicant와 Authenticator 그리고 Authentication Server 간의 인증 및 키 분배 과정을 정의하고 있다. 단말과 같은 Supplicant와 Authentication Server (가령, RADIUS나 DIAMETER)간의 상호인증 과정에서 동적으로 생성된 마스터 세션키는 인증 서버로부터 Authenticator인 AP로 분배된다. 이렇게 분배된 키는 나중에 패킷 단위로 무선 접속 구간의 데이터 프라이버시를 제공하기 위한 기본 키 자체로 쓰이거나 기본 키를 생성하기 위한 Source 키로 사용된다. 또한 Authenticator는 인증이 성공적으로 이루어진 단말에 대해 controlled port를 인가하여 무선 LAN 서비스를 제공한다.

802.1x에서의 인증은 EAP를 가입자 인증 데이터 전송을 위한 표준 프로토콜로 이용하고 있다. EAP는 다중 인증 메커니즘을 지원하는 일반적인 프로토콜로서 스마트 카드, Keberos, 공용키 암호화, OTP(One Time Password)를 포함한 수많은 인증 구조를 지원한다. 또한 802.1x에서는 Supplicant와 Authenticator 사이의 패킷 전송을 위하여 EAPOL(EAP over LAN)이라는 캡슐화 기술을 정의하고 있다. 대표적인 EAP 인증 유형은 (그림 4)와 같으며 특히, EAP-TLS와 EAP-TTLS는 이동 단말과 인증 서버간에 상호 인증을 지원할 수 있는 프로토콜이다.



(그림 4) EAP 인증 유형

802.1x 프로토콜의 동작은 다음 (그림 5)과 같다. 사용자(Supplicnat PAE)가 먼저 접속을 시도하는 경우, EAP-Start 메시지를 AP (authentication PAE)에게 전송한다. AP는 EAP-Start 메시지를 받으면 단말에게 가입자 인증에 필요한 신원(Idnetity) 정보를 요청하는 메시지를 보낸다. 사용자의 신원 정보는 EAP-attribute 형태로 응답 메시지에 담겨 단말로부터 AP를 거쳐 인증 서버(Authentication Server PAE)에 전송된다. 이어 Challenge-Response를 통해 인증이 완료된 후 그 결과에 따라 인증 성공/실패 메시지가 AP에 전송되면 인증 과정이 완료된다. 이때 인증이 성공할 경우 인증 서버는 단말과 관련한 개별 마스터 세션키를 생성하고 이 키를 Radius-Access-Request 메시지에 담아 AP에 전달한다. 전달된 마스터 세션키는 무선 데이터 프라이버시를 보장하기 위한 마스터키(PMK :

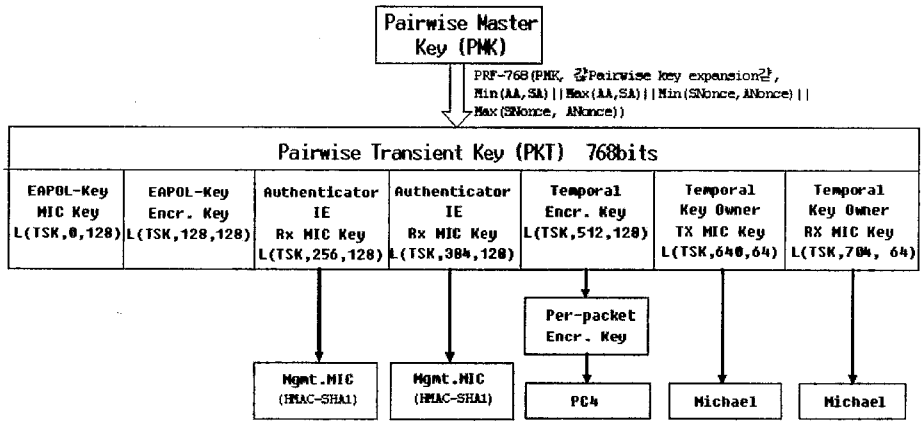


(그림 5) 802.1x 프레임워크를 이용한 무선 LAN 접속과정

Pairwise Master Key)로 불리며, 이 PMK는 cipher suite를 실행하는 데 필요한 키인 PTK(Pairwise Transient Key) 크기로 확대 생성된 후 세부 사용 목적에 따른 크기로 절단되어 사용된다. AP의 키 매니저는 단말과 EAPOL-Key메시지를 통한 키 교환을 수행하여 키 사용 시점을 동기화 한후 EAP-Success 메시지를 단말에 전송하여 802.1x를 이용한 무선 LAN 접속이 허용되었음을 단말에게 알린다.

3.4 Data privacy 메커니즘

인증이 완료된 후 단말과 액세스 포인트는 선택된 암호 알고리즘(WEP, TKIP, AES)을 동작시키는데 필요한 세부 키를 생성하고 EAPOL-Key와 같은 키 교환 프로토콜을 이용하여 상호간 키를 일치시킴으로써 Data privacy를 지원하기 위한 무선 구간의 Security Association을 설정한다. 다음 (그림 6)은 TKIP의 Pairwise 키 계층적 구성도를 나타낸 것이다. 인증 수행 후 Radius-Access-Request 메시지를 통해 AP에



(그림 6) TKIP Pairwise Key Hierarch

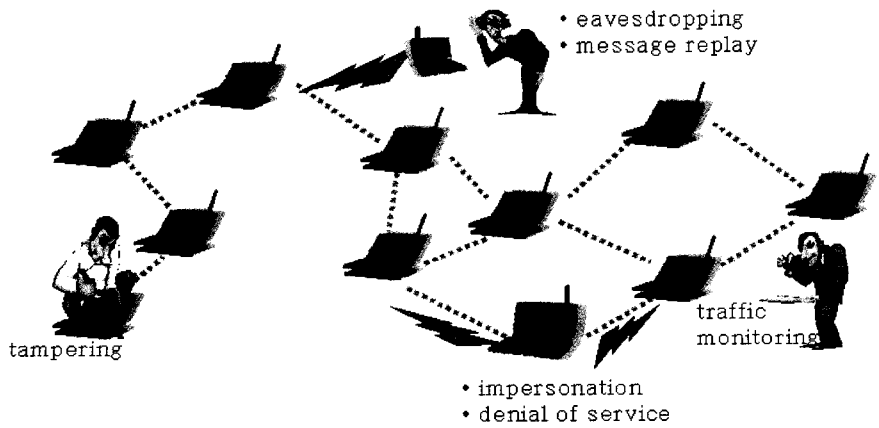
전달된 768 bits의 PMK로부터 PTK가 유도되고 다시 PTK는 EAPOL 암호화키나 TKIP 암호화키 등 7가지의 세부 키로 분해되어 사용된다. 이 세부 키들은 EAPOL 키 교환 과정과 데이터 패킷 송수신 과정의 기밀성과 무결성을 보장하기 위해 사용된다. 키 계층성(Key Hierarchy)이란 루트 키로부터 메시지 암복호화나 인증을 위한 암호화키를 생성해 내는 일련의 절차로서 키 계층으로 마스터키 생성, 키 갱신, 패킷당 암호화 키 생성 등이 있다[6].

TKIP은 기존의 WEP RC4 알고리즘의 보안 문제를 소프트웨어적으로 개선하여 단말과 액세스 포인트에 패치하여 사용할 수 있도록 하는 방식으로서 해쉬를 이용하여 키의 재사용 취약점을 보완하고 메시지의 무결성 체크 및 일련 번호를 부여하여 재실행 공격에 대비하였다. 또한 AES 알고리즘은 매우 불안정한 DES 대신 리즌델(Rijndael) 블록 알고리즘 기반으로 하여 보안성을 높인 블록 알고리즘이다. AES는 블록 길이와 키 길이가 가변적(128, 196, 256)이고 암·복호화가 빠른 대칭 키 알고리즘으로서 Draft에서는 AES 알고리즘을 OCB 모드로 사용하여 기밀성과 데이터 인증을 제공할 수 있도록 하였다. 그러나 AES는 하드웨어 설계상의 변경이 필요하므로 호환상의 문제가 있으나 장기적인 관점에서 TKIP보다 더욱 안정적인 암호화 알고리즘으로 성장할 가능성이 높다.

3.5 무선 LAN Ad hoc 보안 이슈

이동 Ad hoc 네트워크는 공유된 무선 채널을 통해 AP나 기지국과 같은 유선 기반구조의 도움 없이 언제 어디서나 즉석 통신을 가능하게 해준다. 이러한 Ad hoc 네트워크는 무선을 통한 브로드캐스팅 방식의 정보 전달과 중앙 집중적인 인증 및 키 관리 장치의 부재 등의 본질적인 특성으로 인해 여러 가지 보안상 위협에 취약한 면을 지니고 있다. 다음 (그림 7)은 Ad hoc 네트워크상에서의 각 호스트들이 만나게 되는 보안상의 위협들을 나타낸 것이다.

현재 Ad hoc 망에서 제기되고 있는 보안 이슈들에 대해 다양한 대응책들이 제안되고 있다. 잘못된 라우팅 정보의 삽입, 라우팅 정보의 파괴, 중계기능의 고의적인 비수행 등과 같은 라우팅 공격에 대한 안전성을 보장하기 위한 기술로 다중의 라우팅 경로 특성을 이용하는 방안이 제안되었고, Ad hoc망에서도 인증, 기밀성, 서명, 부인봉쇄 등의 보안 서비스를 제공하기 위해 Ad hoc 네트워크의 특성에 적합한 키 관리 프로토콜을 설계하



(그림 7) Ad hoc 네트워크의 위협요소

기 위한 연구들이 현재 활발히 진행되고 있다. 이 때 사용되는 키 관리 프로토콜로는 기존의 유선에서 사용되는 Diffie-Hellman 프로토콜, 하이퍼큐브 프로토콜을 응용하여 위상변화가 적고 공개키 기반 보안을 수행하기에 부하가 큰 단말에 대해 대칭 키 관리 방식[7][8]을 수행하거나 인증기관(Certification Authority)의 기능을 적절히 분산시켜 협력작업을 통해 공개키 관리[9][10]를 수행하는 등 다양한 보안 방법들이 제안되고 있다.

최근 무선 LAN이나 이동통신망의 보안을 위한 주요 제반 보안 기술로 무선 PKI(Public Key Infrastructure)가 제도적, 기술적으로 틀을 잡고 있다. Ad hoc 네트워크의 보안에 관한 연구는 라우팅과 키 관리에 관한 프로토콜들을 표준화하지 않은 채 다양한 Ad hoc 프로토콜의 특성에 맞게 보완하고 수정하는 방식으로 진행되어 왔다. 따라서 Ad hoc 네트워크와 무선 LAN과의 자연스런 통합 및 운영을 위해서는 무선 LAN Ad hoc 네트워크에서 운영이 가능하고, 기존의 유선 기반 네트워크와의 자연스런 통합을 위한 Ad hoc 환경에 맞는 공개키 기반구조의 재정 및 수정이 요구된다. 이러한 통합 공개키 기반구조를 통해 무선 LAN의 서비스 영역에서는 무선 LAN에서 제공하는 보안 서비스를 이용하고, 긴급하고 즉시성이 요구되는 통신환경에서는 Ad hoc 보안 서비스를 이용하는 지속적인 보안 서비스 이용이 가능할 것이다.

3.6 무선 LAN 보안 기술의 확장

전문에서 살펴본 바와 같이 802.11i WG에서는 향상된 보안 구조로 RSN의 표준화를 진행중이며, 그 밖에 Wi-Fi에서도 WEP 대체 보안 표준으로 WPA(Wi-Fi Protected Access)을 발표하였다. 또한 이와 같은 표준 기술들을 탑재한 다양한 칩 기반 무선 LAN 제품들이 출시될 예정에 있다. 그러나 이와 같은 표준 기술에 전적으로 의존하지 않고 보안 솔루션 보급의 시간 지연 문제를 완화하고 네트워크 제반 사항에 맞게 능동적으로 무선 LAN 보안 취약점을 개선하기 위하여 다양한 무선 LAN 보안 확장 기술들이 제안되고 있다.

그 중 하나로 IPSec-VPN(Virtual Private Network)의 연계를 들 수 있다. 이 방식은 무선 LAN을 방화벽 밖에 두고 VPN 서버를 통한 인증과 암호화를 제공해 사용자가 기업의 사내망과 같은 내부망에 접속할 수 있게 한다. 구축에 있어 추가비용 및 관리비용을 더 감수해야 하고, 멀티캐스트와 같은 서비스 지원이 어렵다는 단점을 안고 있지만 WEP이 갖고 있는 근본적인 문제를 피할 수 있는 확실한 방법이라고 할 수 있다. VPN 서버를 게이트웨이로 사용하는 것은 사용자 인증뿐 아니라 모든 무선 LAN 트래픽이 사용자 고유의 키로 암호화되기 때문에 WEP 공유키를 사용할 필요가 없으며 IPSec 프로세스의 일부로 사용자 인증과 권한 부여 등의 이점도 얻을 수 있기 때문이다[11]. VPN이 유용하지 않은 경우에는 무선 LAN 계층에서 더 강력한 암호화를 요구하는 애플리케이션을 위해 AMSA(Advanced Mobile Security Architecture)의 도입도 가능하다. AMSA는 WEP이 갖고 있는 여러 취약점을 극복하기 위해 128bit 암호체계인 RC4 기법을 사용한다. 즉 AMSA는 128bit로 사용자마다 다른 두 개의 개인적인 보안 터널을 만들기 때문에 매우 높은 수준의 보안 기능을 지원한다[12]. 이 밖에도 동적인 다이내믹 WEP 키를 생성할 수 있는 TLS, TTLS 등과 인증서버를 사용하는 방법을 병행하거나 SSL이나 VLAN과 연계하는 등의 무선 LAN 보안성을 높이기 위한 노력은 다양하게 전개되고 있다.

4. 결 론

이동성은 적지만 빠른 전송 속도와 높은 대역폭

지원을 가능케 하는 무선 LAN 제반 기술의 향상과 이동 장치의 급속한 보급으로 무선 LAN 서비스가 증대되고 있을 뿐 아니라 앞으로 고정 무선 인터넷 서비스에서 발전되어 Mobile IP 기반의 이동 인터넷 서비스 제공으로까지 기술이 발전 될 것으로 예상된다. 그러나 이와 같은 무선 LAN의 활성화에 반하여 현재 나와 있는 무선 LAN 보안 방법은 많은 부분 보안상 결함을 안고 있으며 무선 LAN 사용자나 공급자들 또한 보안에 대해 상당부분 무관심하다. 최근 테헤란로 일대의 IT 기업 중 WEP을 작동시키며 운영하고 있는 AP의 숫자는 탐지된 AP 총 287개중 65개뿐이어서 WEP 구동률 22.6%에 불과 했다는 전자신문의 조사가 이를 뒷받침하고 있다.

따라서 무선 인터넷 사업자(WISP)들은 무선 LAN 서비스의 보급 뿐 아니라, 보다 안전한 무선 LAN 서비스를 제공하기 위해 책임감을 갖고 표준 보안 프로토콜의 준수에 신경써야 하며 더 나아가 더욱 개선된 무선 LAN 보안 솔루션들을 개발하기 위해 꾸준히 연구를 수행해야 한다. 아울러 액세스 포인트 공유를 통한 무선 인터넷 사업자간이 무선 LAN 로밍 및 이동 보안을 위해 분산 인증 및 실시간 패킷 과금, 무선 LAN Ad hoc 망에 대한 보안 연구가 더욱 활성화 되어야 한다.

참고문헌

[1] 간태경, "2003년 54Mbps 무선랜 등장으로 제 2의 성장기 도래," NETWORK TIMES, Dec. 2002

[2] M. M. Gast, "Seven Security Problems of 802.11 Wireless," O'Reilly Network, May, 2002

[3] A. Mishra, "An Initial Security Analysis of the IEEE 802.1x Standard," CS-TR4328, University of Maryland, Feb. 2002

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

[5] IEEE Draft, "IEEE P802.11 Wireless LANs: Proposed TGi D1.8 Clause 8 Editing Changes," IEEE 802.11-02/178r0, Mar, 2002

[6] IEEE Draft, "IEEE P802.11 Wireless LANs: IEEE 802.1x Pre-Authentication," IEEE 802.11-02/TBDr0, May, 2002

[7] N. Asokan, et al., "Key Agreement in Ad-hoc Networks, Computer Communication Review, 23 (17), pp. 1627-1637, 2000

[8] S. Basagni, et al., "Secure Pebblenets," ACM Symp. on MobiHoc, 2001, pp. 156-163

[9] S. Yi, et al., "Key Management for Heterogeneous Ad Hoc Wireless Networks," Department of Computer Science, University of Illinois, Urbana-Champaign, Technical Report UIUCDCS-R-2002-2290, 2002

[10] J. Kong, et al., "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE ICNP 2001, 2001

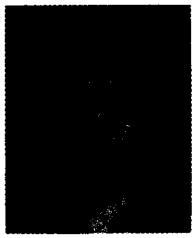
[11] NORTEL NETWORKS White Papter, "Secure Architectures for Wireless LANs in the Enterprise," 2002

[12] J. Haagh, "〈테마특강〉 무선 LAN 보안," 전자신문 May, 2002

저자약력

송 지 은

2002년 전북대학교 컴퓨터과학과 졸업(이학사)
2002년~현재 전북대학교 컴퓨터정보학과(석사과정)
관심분야 : 무선인터넷 보안, AAA, Ad hoc Security, 분산처리시스템
이 메 일 : jeusong@dcs.chonbuk.ac.kr



김 태 연

1986년 전남대학교 계산통계학과 (이학사)
1988년 전남대학교 대학원 전산통계학과 (이학석사)
1996년 전남대학교 대학원 전산통계학과 (이학박사)
1996년~현재 서남대학교 컴퓨터정보통신학과 조교수
관심분야 : 정보보안, 통신망 관리, 이동통신 등
이 메 일 : tykim@tiger.seonam.ac.kr

왕 기 철

1997년 광주대학교 전자계산학과(학사)
2000년 목포대학교 대학원 컴퓨터 과학과(석사)
2001년~현재 전북대학교 컴퓨터 통계 정보학과 박사과정
관심분야 : 이동컴퓨팅, Ad hoc 네트워크의 라우팅 및 보안
이 메 일 : kingkid@dcs.chonbuk.ac.kr

조 기 환

1985년 전남대학교 계산통계학과 졸업(학사)
1987년 서울대학교 계산통계학과 졸업(석사)
1996년 영국 New-castle 대학교 전산학과 졸업(박사)
1987년~1997년 한국전자통신연구원 선임연구원
1997년~1999년 목포대학교 컴퓨터과학과 전임강사
1999년~현재 전북대학교 전자정보공학부 조교수
관심분야 : 이동컴퓨팅, Ad hoc 네트워크, AAA, 컴퓨터통신, 분산처리시스템
이 메 일 : ghcho@dcs.chonbuk.ac.kr