무선랜 보안 표준 IEEE 802.11i

한국전자통신연구원 정보보호연구단 **강 유 성, 오 경 희, 정 병 호, 정 교 일**
TTA 무선랜프로젝트그룹 의장, 한국전파진흥협회 정책연구팀장 **정 찬 형**

요약

초고속 무선인터넷에 대한 요구가 급성장하면서 기존의 무선랜(WLAN: Wireless Local Area Network) 시스템이 초고속 무선인터넷의 기반구조로써 자리잡고 있음은 주지의 사실이다. 그러나 합리적인 가격과 편리성에도 불구하고 보안의 취약성이 문제로 남아있었다. 이 문제의 해결을 위한 노력의 결실로써 IEEE 802.11i 표준은 지난 2004년 6월 24일에 IEEE 802 SEC(Sponsor Executive Committee)의 투표를 통과하여 2004년 7월에 IEEE 표준으로 확정되었다[2]. 또한 신속한 국제표준화를 위해서 ISO/IEC JTC1 Fast Track DIS(Draft International Standard)로 상정되어 2004년 12월 8일부터 최종 승인을 위한 투표를 진행 중이다[5]. 본 고에서는 IEEE 802.11i 무선랜 보안 표준이 담고 있는 인증 방식, 키 교환 방식 및 암호 알고리즘에 대하여 분석해 보고자 한다.

I. 들어가며

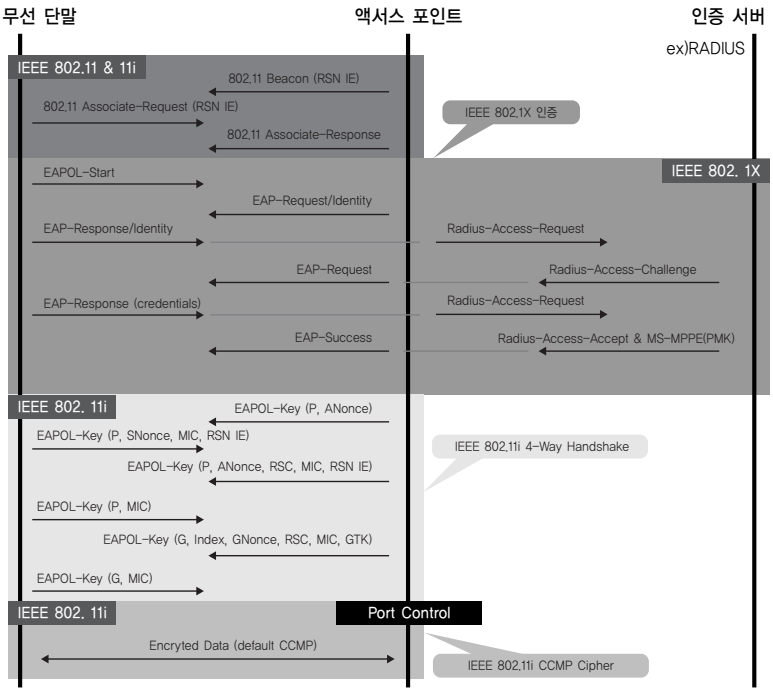
IEEE 802.11 기반의 무선랜 서비스의 보안 요소에는 사용자 인증(Authentication), 접근 제어(Access control), 권한 검증(Authorization), 데이터 기밀성(Confidentiality), 데이터 무결성(Integrity), 부인 방지(Non-repudiation) 및 안전한 핸드오프(Secure handoff) 등이 있으며, 이러한 보안 요소가 전체적으로 만족되었을 때 안전한 무선랜 보안 시스템이라 할 수 있다[1]. 본 고에서는 IEEE 802.11i 표준의 인증 방식, 키 교환 방식 및 암호 알고리즘에 대해 설명하고자 하며, 이를 위하여 다음과 같은 구성을 가진다. II장에서 IEEE 802.11i 표준의 표준화 목표, 표준화 범주 등 간략한 개요를 보이며, III장에서는 IEEE 802.11i 표준의 인증 방식에 대해 설명한다. IV장에서는 키 교환 방식, V장에서 암호 알고리즘을 설명하고 끝으로 VI장에서 본 고의 결론을 맺는다.

II. IEEE 802.11i 표준화 목표

IEEE 802.11 기반 무선랜 표준화의 초기 과정에서 설계했던 WEP(Wired Equivalent Privacy) 알고리즘 기반의 보안 대책이 취약하다는 것이 공개되면서[3,4] 무선랜 보호를 위한 관심이 커져 갔으며, IEEE 802.11 워킹 그룹에서는 2001년 5월부터 IEEE 802.11 워킹 그룹 산하에 TGi(Task Group i)를 결성하여 무선랜 MAC 계층 보안 기능 향상을 위한 표준화를 진행하기 시작하였다.

IEEE 802.11 TGi의 표준화 목표는 하나의 액세스 포인트(AP)가 관할하는 기본 서비스 셋(BSS, Basic Service Set) 안에서 액세스 포인트와 무선 단말(MS, Mobile Station) 사이에 인증과 키 교환 및 무선구간 데이터 보호를 통해 튼튼한 보안망(RSN, Robust Security Network)을 구축하여 무선랜 사용자를 보호한다는 것이다. IEEE 802.11i 표준은 무선랜 사용자 보호를 위해서 사용자 인증 방식, 키 교환 방식 및 향상된 무선구간 암호 알고리즘을 정의하고 있으며, IEEE 802.1X 인증, 4-단계 핸드쉐이크(4-Way Handshake) 키 교환 및 CCMP(Counter mode with CBC-MAC Protocol) 암호 알고리즘을 필수 구현 기능으로 정의함으로써 위와 같은 표준화 목표를 충족시키고 있다.

IEEE 802.11i 표준에서는 사용자 인증과 키 교환의 큰 틀로써 IEEE 802.1X를 사용한다고 규정하고 있으며, 나아가 구체적인 키 교환 방식인 4-단계 핸드쉐이크 방식, 교환된 키의 계층적 사용구조(key hierarchy), 그리고 새로운 무선 구간 암호 알고리즘(cipher suites)의 정의를 포함하고 있다. (그림 1)은 IEEE 802.1X 표준과 IEEE 802.11i 표준이 적용되는 무선랜 보안 접속 흐름도를 보이고 있다. 인증과 키 교환을 완료해서 액세스 포인트를 통한 외부 네트워크 연



(그림 1) 무선랜 보안 접속 흐름도

결이 허가되기 위해서는 IEEE 802.11 접속, IEEE 802.1X 인증, IEEE 802.11i 키 교환, 무선 구간 데이터 암호화가 유기적으로 연결되어야 한다.

III. IEEE 802.11i 표준의 인증 방식

(그림 1)의 두 번째 상자로 표현된 부분이 무선랜 보안 접속의 인증 부분이다. IEEE 802.11i 표준에서는 사용자 인증 방식으로 2가지를 정의하고 있다. 첫째는 IEEE 802.1X 인증 방식으로써 필수 구현 항목이며, 둘째는 사전 공유 키(PSK, Pre-Shared Key) 방식으로써 선택 항목이다. 이러한 방식들은 사용자 인증뿐만 아니라 무선 단말과 액세스 포인트 사이에 교환하게 될 세션 키의 마스터 키를 생성하는 키 관리 방식을 구분하기 때문에 이를 통틀어 인증 및 키 관리(AKM, Authentication and Key Management) 방식이라고 부르기도 한다.

첫 번째 필수구현 항목인 IEEE 802.1X 인증 방식은 IEEE 802.1X 태스크 그룹이 작성하여 2001년 6월에 승인받은 표준으로써 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속 포트에 기반한 접근 제어 기능을 정의하고 있다[6]. 무선랜 시스템에서도 이러한 포트 기반 접근 제어를 통해 무선랜 사용자 인증을 수행할 수 있으며, 무선 구간 보안에 필요한 마스터 키(PMK, Pairwise Master Key)를 전달할 수 있다. 무선랜 시스템에서는 액세스 포인트가 접속 허가자(Authenticator) 역할을 하게 되고, IEEE 802.1X 인증을 수행하기 위해서는 액세스 포인트를 관리하는 네트워크 관리자 영역에 접속 요구 단말에 대한 인증 정보를 가지고 있는 인증 서버(Authentication Server)가 존재하거나 액세스 포인트 자체적으로 인증 서버 기능을 내장하고 있어야 한다.

그러나 2001년 6월 버전의 IEEE 802.1X 표준은 무선 구간의 보안을 위한 키 분배 시점 및 키 분배 여부를 접근 제어에 참조하는 조건을 정의하지 않았기 때문에 IEEE 802.11i 표준에서 규정한 새로운 암호 알고리즘을 위한 암호 키 교환을 지원하지 못하는 문제가 발생하였다. 이를 보완하기 위하여 IEEE 802.1X 표준의 재검토(revision) 작업이 진행되어 2004년 7월에 IEEE 802.1X-Rev Draft 11까지 발표되었는데, 이 문서는 접속 요구 단말에 대한 인증과 더불어 무선 구간 암호 키 분배를 위하여 IEEE 802.11i 표준의 키 서술자(Key Descriptor)의 수용과 포트 제어에 키 분배 결과의 반영을 주요 업그레이드 내용으로 갖고 있다[7]. (그림 1)에서 볼 때, 두 번째 상자의 맨 아래 MS-MPPE(PMK) 부분이 인증 서버가 액세스 포인트에게 마스터 키(PMK)를 전달하는 절차이며, 이 마스터 키를 이용하여 일대일 대칭 키(PTK, Pairwise Transient Key) 교환을 하게 되고 그 결과를 참조하여 포트 제어(Port Control)를 수행한다.

두 번째 인증 방식인 사전 공유 키(PSK, Pre-Shared Key) 방식은 별도의 인증 서버가 필요없는 대신 무선 단말과 액세스 포인트가 미리 특정 키를 공유하고 있어야 한다. 소규모 사무실 또는 가정에서 활용가능한 방식으로써 정해진 의사 난수 함수(PRF, Pseudo-Random Function)에 사전 공유 키를 적용하여 마스터 키를 유도한다. (그림 1)의 두 번째 상자의 과정이 생략되는 효과이며, 이후의 일대일 대칭 키(PTK) 교환과 포트 제어 및 데이터 암호화 통신 등의 절차는 동일하다.

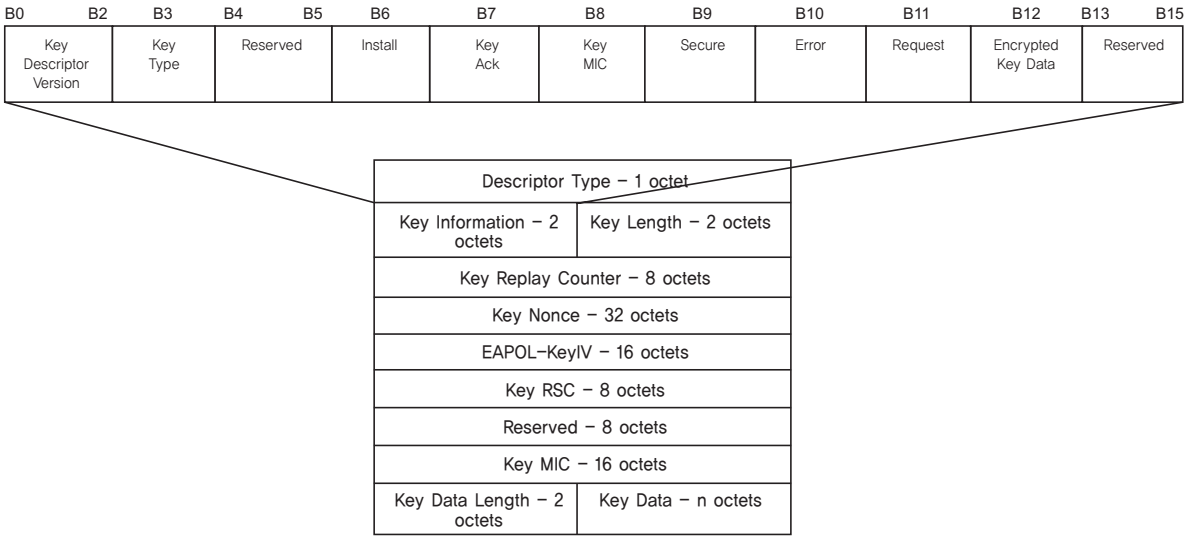
그리고 IEEE 802.11i 표준의 중요한 특징 중의 하나는 선인증(Pre-Authentication) 방식 및 마스터 키(PMK) 관련 정보의 캐시(cache) 기능을 도입한 것이다. 선인증의 기본적인 개념은 무선 단말이 현재 접속된 액세스 포인트뿐만 아니라 인접해 있는 목표 액세스 포인트(Target APs)에게도 인증을 요청해서 미리 다수의 액세스 포인트들로부터 인증을 받아 놓는다는 것이다. 결과적으로 선인증의 최종 단계에서 목표 액세스 포인트는 자신에 직접 접속되어 있지 않은 무선 단말과 관련

된 마스터 키(PMK)를 캐시(cache)하며, 무선 단말은 향후 핸드오프 가능성이 있는 목표 액세스 포인트에게 미리 인증을 받음과 동시에 동일한 마스터 키를 캐시하게 되는 것이다. 그리고, 선인증 결과로써 생성된 마스터 키와 해당 무선 단말의 관계는 마스터 키 인식자(PMKID, PMK Identifier)로써 그 유일성을 확인할 수 있다.

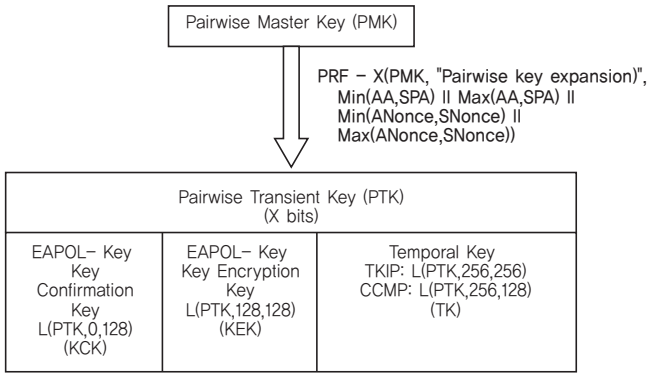
IV. IEEE 802.11i 표준의 키 교환 방식

IEEE 802.11i 표준의 세션 키 교환 방식은 4-단계 핸드쉐이크(4-Way Handshake) 방식으로 대표된다. 그러나 키를 사용하는 대상에 따라 크게 3가지 세션 키가 존재할 수 있으며, 이를 위한 각각의 키 교환 방식으로 세분할 수 있다. 첫 번째는 하나의 무선 단말과 액세스 포인트 사이의 일대일(unicast) 통신 보호용 대칭 키(PTK, Pairwise Transient Key) 교환을 위한 4-단계 핸드쉐이크 방식이고, 두 번째는 액세스 포인트가 다수의 무선 단말과 일대다(broadcast) 통신할 때 사용하는 그룹 키(GTK, Group Transient Key) 교환을 위한 그룹 키 핸드쉐이크(Group Key Handshake) 방식이며, 세 번째는 동일 기본 서비스 셋(BSS) 안에 있는 2개의 무선 단말이 통신할 때 사용하는 단말 대 단말 키(STA to STA key)를 교환하기 위한 단말 키 핸드쉐이크(STAKey Handshake) 방식이다.

동적 키 생성을 위한 4-단계 핸드쉐이크는 (그림 2)와 같은 EAPOL-키 서술자(EAPOL-Key Descriptor)를 이용하여 진행된다. EAPOL-키 서술자는 4-단계 핸드쉐이크 뿐만 아니라 그룹 키 핸드쉐이크와 단말 키 핸드쉐이크에서도 사용된다. 일대일 대칭 키(PTK)를 설립하는 것과 더불어 IEEE 802.11i 4-단계 핸드쉐이크는 MAC 계층에서의 보안 협상을 재확인 또는 변경할 수 있는 기능도 제공한다. 4-단계 핸드쉐이크의 두 번째, 세 번째 메시지는 EAPOL-키 서술자의 키 데이터(key data) 필드에 튼튼한 보안망 정보 요소(RSN IE, Robust Security Network Information Element)를 포함하고 있다. 튼튼한 보안망 정보 요소



(그림 2) EAPOL-Key Descriptor



(그림 3) Pairwise Key Hierarchy

(RSN IE)는 무선 단말과 액세스 포인트 사이의 인증 방식과 암호 알고리즘에 대한 협상 정보를 지닌 메시지로써 무선랜 MAC 접속(association) 단계에서 교환되고 협상된다. 이러한 튼튼한 보안망 정보 요소(RSN IE)를 4-단계 핸드쉐이크 메시지에 포함시킴으로써 MAC 상위 계층에서 튼튼한 보안망 정보 요소(RSN IE) 정보를 재확인하고 해석할 수 있도록 했다.

두 번째, 그룹 키 핸드쉐이크(Group Key Handshake) 방식을 살펴 보면 다음과 같다. (그림 1)의 "IEEE 802.11i 4-Way Handshake"로 표시된 세 번째 상자에 보이는 6개의 교환 절차 중 하위 2개의 교환 절차가 그룹 키 핸드쉐이크를 나타내고 있다.

그룹 키 핸드쉐이크인 경우에는 액세스 포인트에서 일대다 그룹 키(GTK, Group Transient Key)를 생성하여 암호화한 후 EAPOL-키 서술자의 키 데이터(key data) 필드에 실어서 보내면 무선 단말은 자신이 보유하고 있는 EAPOL-키 암호화 키(Key Encryption Key) 정보를 이용하여 복원해 낸다. (그림 3)의 맨 하단의 두 번째 영역이다.

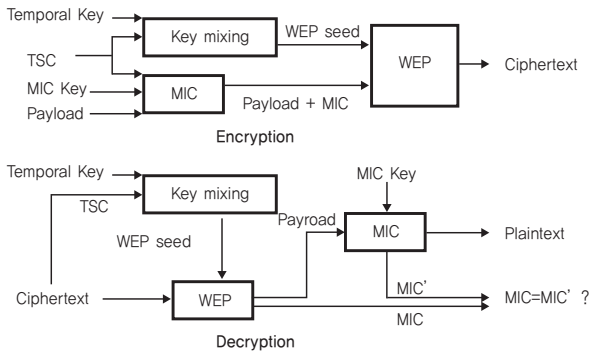
세 번째, 단말 키 핸드쉐이크(STAKey Handshake) 방식을 살펴 보면 다음과 같다. 단말 키 핸드쉐이크의 목적은 동일한 기본 서비스 셋(BSS) 안에 있는 무선 단말끼리 데이터를 주고 받을 때 사용하기 위한 암호 키를 별도로 갖기 위함이다. 무선랜 기반 구조 모드(Infrastructure mode)에서는 모든 무선 단말은 액세스 포인트를 통해서만 네트워크와 연결되므로 액세스 포인트는 모든 무선 단말들로부터 수신한 데이터를 복호화해야 하며, 또한 전달해야 할 데이터가 있는 경우에는 암호화해서 무선 단말에게 송신해야 하는 부담이 있다. 단말 키 핸드쉐이크는 동일 기본 서비스 셋(BSS) 안의 무선 단말끼리 암호 키를 설립하여 해당 암호 키로 암호화한 데이터는 액세스 포인트가 상대편 무선 단말에게 그냥 전달해 줌으로써 액세스 포인트의 암복호화 부담을 줄이는 효과를 얻을 수 있다.

V. IEEE 802.11i 표준의 암호 알고리즘

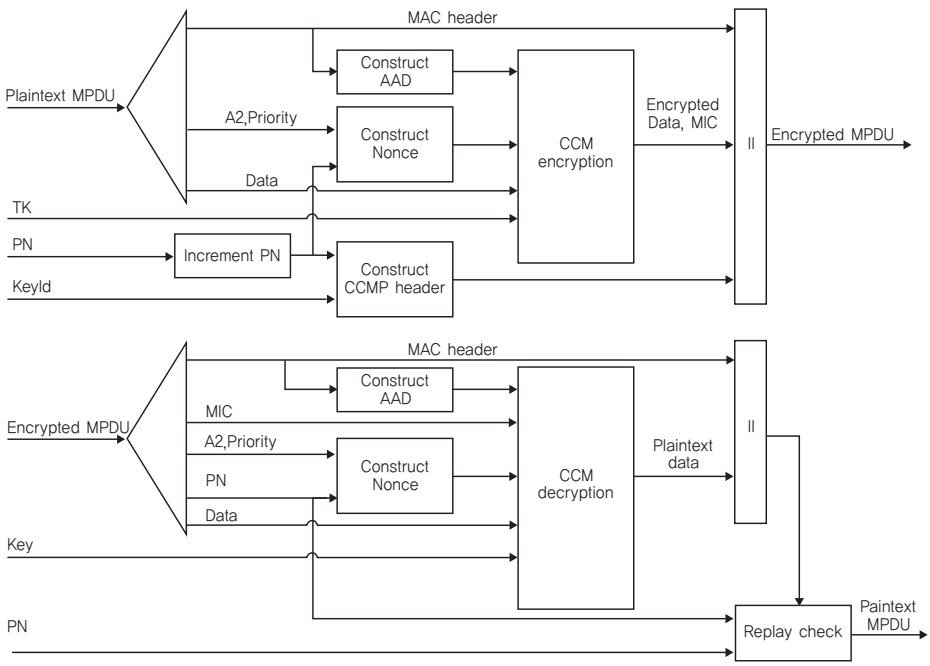
무선 구간 데이터를 보호하기 위한 방법으로 WEP(Wired Equivalent Privacy) 이외에 접속 과정에서 무선 단말과 액세스 포인트 사이에서 설립된 암호 키를 사용하는 TKIP(Temporal Key Integrity Protocol) 알고리즘과 CCMP(Counter mode with CBC-MAC Protocol) 알고리즘이 있다. TKIP은 WEP을 확장하는 방법을 사용함으로써, 기존의 하드웨어 교체가 필요없이 구현할 수 있도록 설계되었다. TKIP에서는 WEP을 이용한 암호화 이전에 별도의 키 생성 과

정을 거치게 하여, WEP에 적용되는 키가 각 데이터 프레임마다 변경되도록 하였다. 그리고, 메시지 무결성 코드인 MIC(Message Integrity Code)를 프레임에 포함시켰다. 이러한 방법으로 WEP 알고리즘의 취약점을 해결하였다. (그림 4)는 TKIP 알고리즘의 암복호화 과정을 보여준다.

CCMP(Counter mode with CBC-MAC Protocol)는 CCM 모드를 사용하는 AES(Advanced Encryption Standard) 암호 알고리즘을 사용한다. (그림 5)는 CCMP 알고리즘의 암복호화 과정을 보여준다.



(그림 4) TKIP 암복호화 과정



(그림 5) CCMP 암복호화 과정

패킷 번호(PN, Packet Number)는 계속 증가하여 동일한 임시 키(TK, Temporal Key)에 중복되지 않도록 하여 재시도 공격(replay attack)을 방지하며, MAC 헤더 정보의 일부인 추가 인증 데이터(AAD, Additional Authentication Data)를 CCM 암호화 과정에 포함시켜 위조를 방지한다.

VI. 맺으며

무선랜 시스템의 최대 단점으로 지적되어왔던 보안 문제를 극복하기 위한 노력으로 IEEE 802.11 TGi가 결성되었으며, 무선랜 보안 기술 표준화에 가장 큰 역할을 하였다. 그 결실로 IEEE 802.11i 표준 문서인 "IEEE 802.11i MAC Security Enhancements" 문서를 완성하였다. IEEE 802.11i 표준은 무선랜 시스템의 보안을 위하여 현존하는 다양한 기술을 통합할 수 있도록 하고 있으며, 또한 새로운 키 교환 방식과 암호 알고리즘을 정의하고 이러한 내용들을 적절하게 조화(coordination)시켜 그 효과를 극대화하고 있다.

IEEE 802.11i 표준은 무선 단말의 고정 통신에 대해서는 효과적인 보안 기능을 제공하지만 향후에 보다 완전한 무선랜 시스템의 보안을 위해서는 무선 단말의 신속하고 안전한 이동성을 보장하는 이동 보안 측면에서는 더욱 발전된 기술이 필요하다. 선인증(pre-authentication)과 마스터 키(PMK) 관련 정보의 캐시(cache)가 이동 보안을 위한 기초적인 기능을 제공하고 있지만 이는 실시간 핸드오프를 요구하는 VoIP(Voice over IP) 등의 응용에서는 보완이 필요할 것으로 보인다. 그리고 무선랜 보안을 위하여 반드시 고려해야 할 또 다른 사항은 관리 프레임(management frame)을 효과적으로 보호하는 방법이다. 관리 프레임의 취약성으로 기인한 공격을 방어할 수 있고, IEEE 802.11i 표준이 요구하는 보안 강도를 유지하면서 액세스 포인트 사이를 신속하게 이동할 수 있는 기술 개발은 또 다른 과제이며 보다 향상된 서비스를 제공할 미래 기술이 될 것이다.

참고문헌

[1] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화동향 및 전망", 전자통신동향분석, 제 18권 제 4호, pp. 36-46, 2003년 8월.

[2] IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Std 802.11i, July 2004.

[3] J. R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", Tech. Rep. 03628, IEEE 802.11 committee, March 2000.

[4] W. A. Arbaugh, N. Shankar, and Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, December 2001.

[5] ISO/IEC, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific

requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", Draft Amendment ISO/IEC DIS 8802-11/Amd.6, ANSI/IEEE Std 802.11i, December 2004.

[6] IEEE, " Standard for Local and metropolitan area networks- Port-Based Network Access Control", IEEE Std 802.1X, June 2001.

[7] IEEE, "DRAFT Standard for Local and Metropolitan Area Networks- Port-Based Network Access Control(Revision)", IEEE P802.1X-REV/D11, July 22, 2004. TTA