

무선 LAN 보호를 위한 IEEE 802.11 표준안에 관한 연구

(A study on IEEE 802.11 for wireless LAN security)

신영환 박영호
(Young-Hwan Sin) (Young-Ho Park)

요약 휴대용 컴퓨터의 보급이 확산됨에 따라 이들을 장소에 상관없이 컴퓨터망에 연결시키는 수단으로 무선 LAN의 사용이 확산되고 있으나 무선 LAN 서비스는 전파라는 무선매체를 사용함으로써 정보도용의 가능성이 높으며 감지도 어렵다는 특징을 가지므로 정보보호가 요구된다. 본 논문에서는 IEEE 802.11 표준안 및 IEEE 802.11eS 초안에서 제시하는 무선 LAN의 정보보호기술인 ESN, WEP, AES 및 SMIB에 관하여 기술한다.

1. 서론

최근 휴대용 컴퓨터의 보급이 확산됨에 따라 이들을 장소에 상관없이 컴퓨터망에 연결시키는 수단으로 무선 LAN의 필요성이 증대되고 있다. 무선 LAN은 무선전송 기술을 사용하여 기존의 유선 LAN의 미비점을 보완하고 유선 LAN의 설치가 어려운 환경까지 무선채널을 통해 LAN을 확장시킬 수 있는 이동성, 휴대성 및 간편성 등의 이점으로 응용분야가 확산되고 있다.^[1,2] 무선 LAN에 대한 국제 표준화는 1990년 10월부터 IEEE 802.11 위원회에 의해 무선 MAC(media access control)와 물리 계층 규격에 대한 표준화가 OSI 참조 모델에 준하여 진행되고 있으며 무선 멀티미디어 서비스 요구의 증가와 무선 전송 기술의 발달로 인하여 1~2 Mbps 전송속도를 갖는 무선 LAN의 표준안인 IEEE 802.11^[3] 규격을 향상시켜 2.4GHz 대에서 1~11 Mbps의 전송속도를 갖는 IEEE 802.11b 표준안^[4]을 5 GHz 대에서 6~54 Mbps의 전송속도를 갖는 IEEE 802.11a 표준안^[5]을 제시하였다.

무선 LAN 서비스는 전파라는 무선매체를 사용함으로써 이동성, 휴대성 등의 편리성을 제공하는 반면 정보도용의 가능성이 높으며 감지도 어렵다는 특징을 가지므로

정보보호가 요구된다. IEEE 802.11 표준안에서는 무선 LAN에서의 정보를 보호하기 위하여 WEP(wired equivalent privacy) 방식을 사용하였다. WEP에서는 초기 백터 IV를 변경함으로써 발생하는 키를 사용하므로 brute-force에 의한 비밀키 획득이 어려우며 각 메시지에 대하여 자기동기가 가능하며 하드웨어 및 소프트웨어적으로 구현이 쉽다는 장점이 있다. 또한, WEP은 평문이 동일한 길이의 의사잡음 키열과 비트별 XOR 연산을 수행함으로써 암호문을 발생한다. IEEE 802.11eS 초안^[6]에서는 기존 WEP 방식에서 사용된 키와 IV 값이 작아서 암호학적인 정교한 공격에는 보호를 제공할 수 없고 데이터 변형 및 재사용을 막을 수 없으므로 128비트 암호화 키와 IV를 사용하도록 제시하였다. 또한, 무선 LAN에서의 인증과 키 관리 서비스를 제공하기 위하여 MAC 계층 위에 ESN(enhanced security network) 프로토콜을 적용하였으며 AES(advanced encryption standard) 알고리즘을 제시하였다. AES 알고리즘은 반복된 블록 암호화인 Rijndael에 기초하며 구현은 선택사항이나 ESN을 제공시에는 AES를 구현해야 한다. ESN을 위해 선택된 AES 동작 모드는 OCB(offset codebook) 모드이다. OCB 모드는 데이터 스트림을 암호화함으로써 데이터 보호를 MIC(message integrity code)를 계산함으로써 데이터 무결성을 제공하는 효율적인 방식이다.

본 논문에서는 IEEE 802.11 표준안 및 IEEE 802.11eS 초안에서 제시하는 무선 LAN의 정보보호기술에 관하여

* 상주대학교 대학원 전자전기공학과
** 상주대학교 전자전기공학과 부교수

기술하며 구성은 다음과 같다. 2장에서는 IEEE 802.11 무선 LAN의 일반적인 구조 및 서비스에 관하여 기술하고 3장에서는 IEEE 802.11 표준안의 WEP에 IEEE 802.11eS draft에서 제시한 기능을 부가하여 WEP을 기술하며 4장에서는 AES 알고리즘의 동작을 기술하고 5장에서는 무선 LAN에서 사용될 보호관리정보인 SMIB에 관하여 기술한다. 마지막으로 6장에서는 결론을 맺는다.

II. 무선 LAN 구조

무선 LAN은 기존의 유선 LAN과는 다른 다음과 같은 특성들을 갖는다.

- 1) 수신주소가 수신위치와 같지 않다.
- 2) 무선 LAN에 사용된 물리계층은 유선 미디어와는 다르다.
- 3) STA이 이동국이다.
- 4) 무선 LAN 네트워크는 MAC 부계층 내에서 STA의 이동성을 다루며 상위계층인 LLC 계층은 유선 LAN과 같이 IEEE 802.2를 사용한다.

그림 1은 IEEE 802.11의 구조를 나타낸 것이다. IEEE 802.11 구조는 상위계층에 투명하게 STA의 이동성을 지원하는 무선 LAN을 제공토록 여러 요소들로 구성된다. BSS(basic service set)는 IEEE 802.11 LAN의 기본 구조 블록으로 BSS의 구성 STA간 서로 통신한다. 만약, 한 STA이 BSS로부터 이탈하면 그 STA는 이전 BSS의 다른 구성 STA들과 직접 통신할 수 없게 된다. IBSS(independent BSS)는 IEEE 802.11 LAN의 기본적인 형태로 그림 1에서는 두 개의 IBSS(BSS1, BSS2)를 나타내고 있다. STA들은 전원을 켜거나 끌 수 있으며 STA들이 BSS 범위내에 들어오거나 나갈 수 있으므로 STA와 BSS 사이의 연결은 동적이다. DS(distribution system)는 BSS들을 서로 연결하는데 사용되는 요소이다. DS는 이동 장치가 목적지 주소를 다루는데 필요한 논리적 서비스들과 많은 BSS들을 합치는 것을 가능하게 한다. AP(access point)는 DS로 접근을 제공하는 STA이며 데이터는 AP를 통하여 BSS와 DS 사이를 이동한다. DS와 BSS들은 임의의 크기와 복잡도의 무선 네트워크를 만들 수 있으며 이와 같은 형태의 네트워크를 ESS(extended service set) 네트워크라 한다. 한 ESS 내의 STA들은 서로 통신할 수 있고 이동국들은 같은 ESS 내의 한 BSS로부터 다른 BSS로 LLC에 투명하게 이동할 수 있다. Portal는 비IEEE 802.11 LAN으로부터의 MSDU들이 IEEE 802.11로 들어가는 논리적인 지점이다. Portal

는 IEEE 802.11 구조와 유선 LAN들 사이에 논리적인 통합을 제공한다.

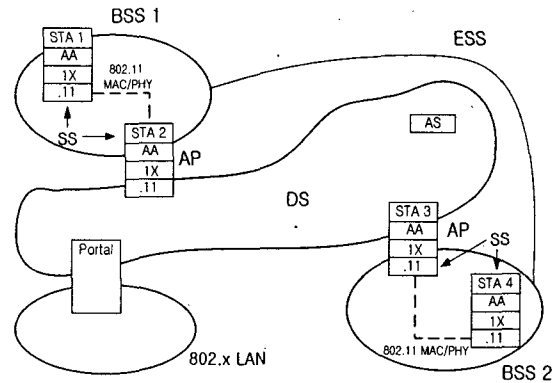


그림 1. IEEE 802.11 architecture.

ESN은 인증과 키 관리 서비스를 제공하기 위하여 IEEE 802.11 MAC 계층 위의 프로토콜들을 사용한다. ESN은 IEEE 802.11 구조에 새로운 요소들을 도입한다. 첫 번째 구성 요소는 IEEE 802.1X 포트이다. IEEE 802.1X 포트들은 ESN에서 모든 STA들에 존재하고 MAC 상위계층에 있으며 MAC를 통해 흐르는 모든 데이터는 IEEE 802.1X 포트를 통과한다. 두 번째 구성요소는 AA(authentication agent)이다. AA는 각 STA에서 IEEE 801.1X 포트 위에 존재하며 인증과 키 관리를 제공한다. 세 번째 구성요소는 AS(authentication server)이다. AS는 ESS에서 모든 STA의 인증에 참가한 엔티티로 DS에 존재한다. AS는 ESN 자체의 엘리먼트들을 인증할 수 있거나 ESN 엘리먼트들이 서로 인증하는데 사용할 수 있는 유형을 제공할 수 있다. AS는 각 STA에 있는 AA와 통신하며 ESS와 STA 사이의 상호 인증은 ESN의 중요한 기능이다.

IEEE 802.11 MAC, IEEE 802.1X 와 ULAP(upper layer authentication protocols)는 ESN STA를 구현하기 위하여 함께 동작한다. ESN에서 MAC는 패킷 필터링과 인증을 관여하지 않는다. IEEE 802.1X 포트는 IEEE 802.11 네트워크를 통하는 데이터 트래픽을 조정한다. ESN에서 AP는 연결된 STA를 위해 IEEE 802.1X 포트를 유지한다. 각 STA에서의 IEEE 802.1X 포트는 AP에 STA의 연관된 포트를 경유하여 로컬 AA와 AS사이의 ULAP 인증 교환을 허가한다. 단지 STA와 AP가 서로 인증한 후에 IEEE 802.1X 포트들은 데이터 트래픽을 가능하게 한다. IEEE 802.1X 포트가 데이터 트래픽을 가능하게 하는 메커니즘은 ULAP에 의존한다.

IEEE 802.11에서 제공하는 서비스들은 연결, 해제, 분배, 통합, 재연결, 인증, deauthentication, 데이터 인증, 키 분배, 프라이버시, 재사용 방지 그리고 MSDU 전달이다. 이 서비스들은 STA에서의 서비스와 DS에서의 서비스로 분류된다. STA에서 제공되는 서비스들은 인증, 데이터 인증, deauthentication, 키 분배, 프라이버시, 재사용 방지 및 MSDU 전달이며 DS에서 제공되는 서비스들은 연결, 해제, 분배, 통합 및 재연결 이다. 이 12개의 서비스들 중 연결, 해제, 분배, 통합, 재연결 및 MSDU 전달 서비스들은 STA간 MSDU 이동을 지원하는데 사용되고 다른 6개의 서비스는 접근제어와 기밀성을 제공하는데 사용된다.

DS 내에서 메시지를 이동하기 위하여 분배 서비스는 어떤 AP가 주어진 IEEE 802.11 STA에 대해 접근하는지를 아는 것이 필요하며 연결 서비스는 이 정보를 DS에게 제공한다. 분배 서비스는 ESS 내에서 동작하는 IEEE 802.11 STA간의 모든 데이터 메시지에 적용되며 해제 서비스는 현재 연결이 끝날 때 사용된다. 통합 서비스는 DSM(distribution system medium)로부터 통합된 LAN 매체로 메시지를 이동하는데 필요한 것을 제공하고 재연결 서비스는 한 AP로부터 다른 AP로 현재의 연결을 이동할 때 사용된다.

인증 서비스는 모든 STA들이 통신하고자 하는 STA에 식별자를 설립하도록 함으로써 사용되며 무선 LAN의 접근을 제어할 수 있다. IEEE 802.11은 STA간 링크레벨 인증을 지원하며 ESN을 사용시 상위계층 인증을 지원할 수 있다.

Deauthentication 서비스는 인증이 끝날 때 사용된다. 데이터 인증 서비스는 수신된 데이터가 패킷의 송신주소 영역에 정의된 MAC 주소인 STA로부터 보내졌다는 것을 확인하는 것이며 AES 알고리즘을 사용하는 STA에서만 사용 가능하다. 키 분배 서비스는 프라이버시, 데이터 인증, 재사용 방지 등의 서비스에서 요구되는 키를 분배하는 것이다. 프라이버시 서비스는 IEEE 802.11에서 메시지 내용을 암호화하는 기능을 제공하며 WEP과 AES 알고리즘들을 사용한다. 재사용 방지 서비스는 수신한 데이터 패킷이 과거에 보낸 패킷의 재전송이 아니라는 것을 확인하는 것이며 AES 알고리즘을 사용하는 STA에서만 사용 가능하다.

그림 2는 IEEE 802.11 참조모델을 나타낸 것이다. 이 참조모델에서는 물리계층, MAC 부계층, 802.1x 부계층으로 정의하였으며 ISO의 OSI 참조모델과의 관계 및 관리 엔티티와의 관계는 그림 2와 같다.

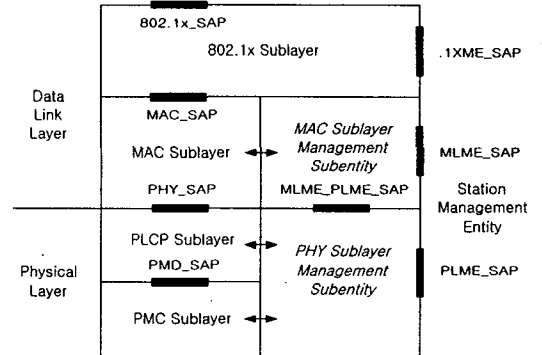


그림 2. Portion of the ISO/IEC reference model covered in IEEE 802.11.

III. WEP

IEEE 802.11은 무선 LAN에서의 인가된 사용자를 보호하기 위하여 WEP 방식을 사용하고 있다. WEP에서는 초기벡터 IV를 변경함으로써 발생하는 키를 사용하므로 brute-force에 의한 비밀키 획득이 어려우며 각 메시지에 대하여 자기동기가 가능하며 하드웨어 및 소프트웨어적으로 구현이 쉽다는 장점이 있다. 또한, WEP의 구현 및 사용은 IEEE 802.11의 선택사항이다. WEP은 Vernam 암호화 형태이며 평문은 동일한 길이의 의사잡음 키열과 비트별 XOR 연산을 수행함으로써 암호문을 발생한다.

그림 3은 WEP 암호화 과정을 나타낸 것이다. 비밀키는 IV와 비트별 XOR하며 결과 seed 값은 PRNG(pseudo random number generator)에 입력된다. 비밀키와 IV는 128.비트이며 비밀키가 128 비트보다 작은 경우 나머지 영역은 0으로 채워지며 128 비트보다 큰 경우는 잘라낸다. PRNG의 출력은 데이터 octet의 길이와 같은 의사잡음 octet의 키열이다. 비인가된 데이터 변경을 막기 위하여 무결성 알고리즘을 평문에 적용하여 4 octets의 ICV 값을 발생한다. 암호화는 발생한 키열과 평문 및 ICV 값을 XOR 연산을 함으로써 이루어지며 암호화 과정의 출력값은 IV와 암호문이다. WEP PRNG는 비교적 짧은 길이의 비밀키를 입력하여 비교적 긴 키열을 발생하는 암호화과정의 중요한 요소이다. IV는 비밀키의 수명을 연장시키고 알고리즘의 자기동기 성질을 제공한다. IV가 주기적으로 바뀔동안 비밀키는 불변이다. 새로운 IV값은 새로운 seed와 키열을 발생하며 IV와 키열간에는 일대일 상관성이 있다. IV는 매 MPDU에 대해 값이 바뀔 수 있으며 IV 값은 메시지와 함께 전송되므로 수신자는 어떠한 메시지도 복호할 수 있다. IV는 비밀키에 관한 어떠한 정보도 가지고 있지 않으며 복호를 위해서 수신자에게 알려져야 하므로 평문으로 전송된다.

그림 4는 WEP 복호화 과정을 나타낸 것이다. 수신 메

시지의 IV 값은 수신 메시지를 복호하는데 필요한 키열을 발생하는데 사용된다. 암호문과 키열의 XOR 연산 결과는 평문과 ICV를 나타낸다. 정확한 복호는 수신된 평문에 무결성 검사 알고리즘을 수행함으로써 이루어진다. 만약, 메시지와 함께 수신된 ICV와 수신측에서 계산한 ICV'가 같지 않으면 수신 MPDU에는 에러가 있으며 에러 표시 값을 MAC 관리 계층에 전송하며 에러가 발생한 MPDU는 LLC 계층에 보내지 않는다.

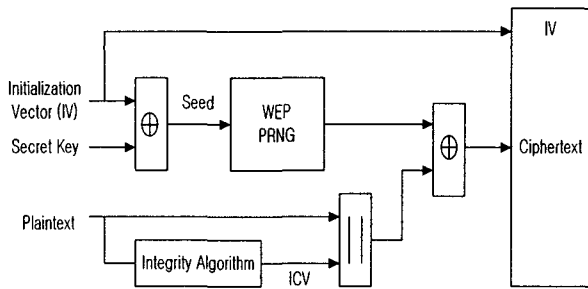


그림 3. WEP encipherment block diagram.

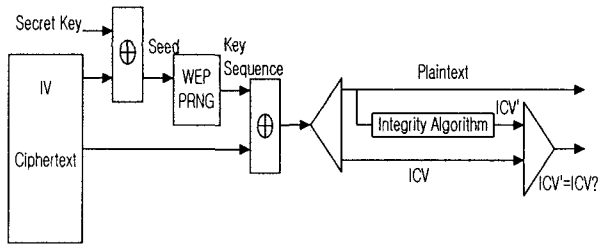


그림 4. WEP decipherment block diagram.

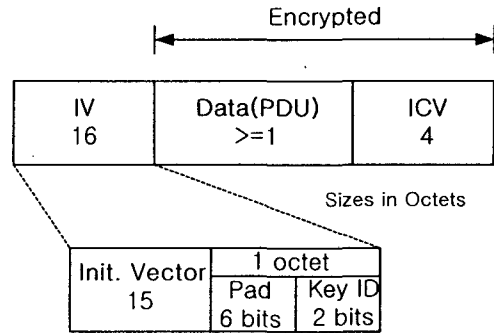


그림 5. WEP frame.

그림 5는 WEP 알고리즘에 의해 구성된 암호화된 프레임의 구조를 나타낸 것이다. ICV 영역은 32 비트이며 무결성 검사 알고리즘은 CRC-32를 사용한다. 128 비트 IV는 120 비트의 IV, 2 비트의 Key ID 및 6 비트의 pad 영역으로 구성된다. Key ID 값은 프레임을 복호하는데 사용할 4개의 가능한 비밀키 중 하나를 선택하는데 사용되며 pad 영역은 0으로 채워진다.

IV. AES

AES 알고리즘은 WEP을 제공하기 위한 선택으로 채택되어진다. AES 알고리즘은 반복된 블록 암호화인 Rijndael에 기초하며 구현은 선택사항이나 ESN을 제공시에는 AES를 구현해야 한다. ESN을 위해 선택된 AES 동작 모드는 OCB 모드이다. OCB 모드는 데이터 스트림을 암호화함으로써 데이터 보호를 MIC를 계산함으로써

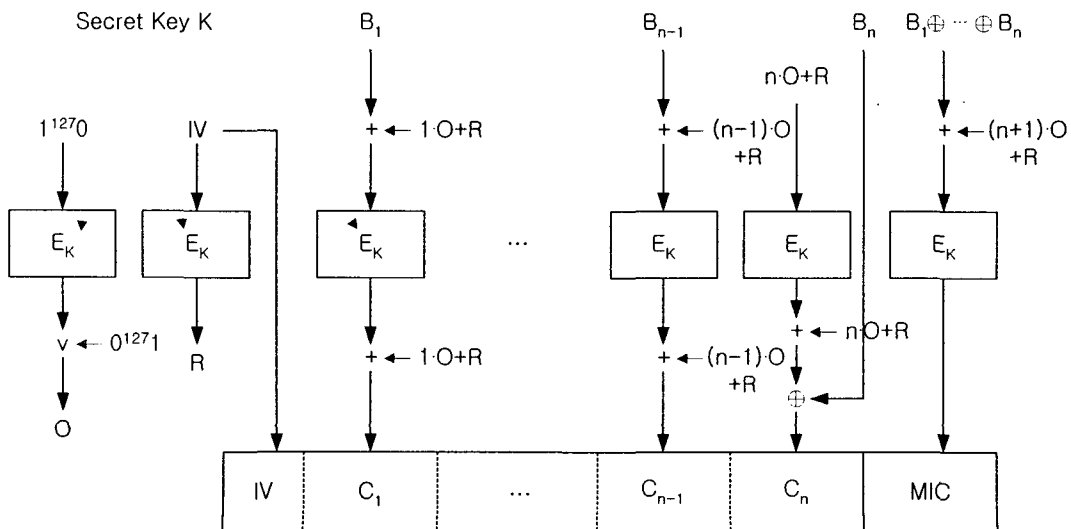


그림 6. AES encipherment block diagram.

데이터 무결성을 제공하는 효율적인 방식이다. OCB 모드는 n 블록의 데이터를 암호화하고 MIC를 추가하는데 n+2 번의 암호화 과정이 요구되며 수신측에서 데이터를 복호하고 무결성을 검사하는데 n+2 번의 복호화 과정이 요구된다. 그림 6은 AES 암호화 블록 다이어그램을 나타낸 것이다. 암호화에 사용되는 offset O는 식 (1)과 같이 발생한다.

$$O = AES_EncryptK(1^{127}0) \vee 0^{127}1 \quad (1)$$

식 (1)에서 $1^{127}0$ 는 비트 스트링의 MSB 및 127개 비트는 1이며 LSB는 0을 나타낸 것이다. Offset O는 키 K가 발생될 때 계산되며 키가 변할 때까지 사용된다. 초기벡터 IV는 128비트이며 식 (2)와 같이 암호화 과정을 거쳐 R을 발생한다.

$$R = AES_EncryptK(IV) \quad (2)$$

R과 offset O는 암호화 전후과정에서 사용된다. OCB 모드 암호화는 데이터를 128비트 블록으로 분리하며 $i = 1 \dots n-1$ 번째까지의 블록 데이터는 식 (3)과 같이 암호화된다.

$$C_i = R + i \cdot O + AES_EncryptK(R + i \cdot O + B_i) \quad (3)$$

마지막 블록이 128 비트이면 식 (4)와 같이 암호화되며 마지막 블록이 128 비트보다 작다면 식 (5)와 같이 암호화된다.

$$C_n = (R + n \cdot O + AES_EncryptK(R + n \cdot O)) \oplus B_n \quad (4)$$

$$C_n = B_n \oplus Mask_{mn}(R + n \cdot O + AES_EncryptK(R + n \cdot O)) \quad (5)$$

식 (5)에서 $Mask_{mn}(A)$ 는 A의 m+1에서 n번째 까지의 비트를 마스크 한다는 것을 의미하며 \oplus 는 비트별 XOR를 의미한다. MIC는 마지막 블록이 128 비트일 때 식 (6)과 같이 계산되며 마지막 블록이 128 비트보다 작다면 식 (7)과 같이 계산된다.

$$MIC = AES_EncryptK((B_1 \oplus B_2 \oplus \dots \oplus B_n) + R + (n+1) \cdot O) \quad (6)$$

$$MIC = AES_EncryptK((B_1 \oplus B_2 \oplus \dots \oplus B_{n-1} \oplus Pad_{mn}(B_n)) + R + (n+1) \cdot O) + R + (n+2) \cdot O \quad (7)$$

식 (7)에서 $Pad_{mn}(A) = 0^{n-m-1}A$ 이다. 그림 7은 AES 복호화 블록 다이어그램을 나타낸 것이다. 각 블록 B_i 는 식 (8)과 같이 복호된다.

$$B_i = AES_DecryptK(C_i - (R + i \cdot O)) - (R + i \cdot O) \quad (8)$$

마지막 블록 B_n 이 128 비트이면 식 (9)와 같이 복호되며 128 비트보다 작으면 식 (10)과 같이 복호된다.

$$B_n = B_n \oplus (R + n \cdot O +$$

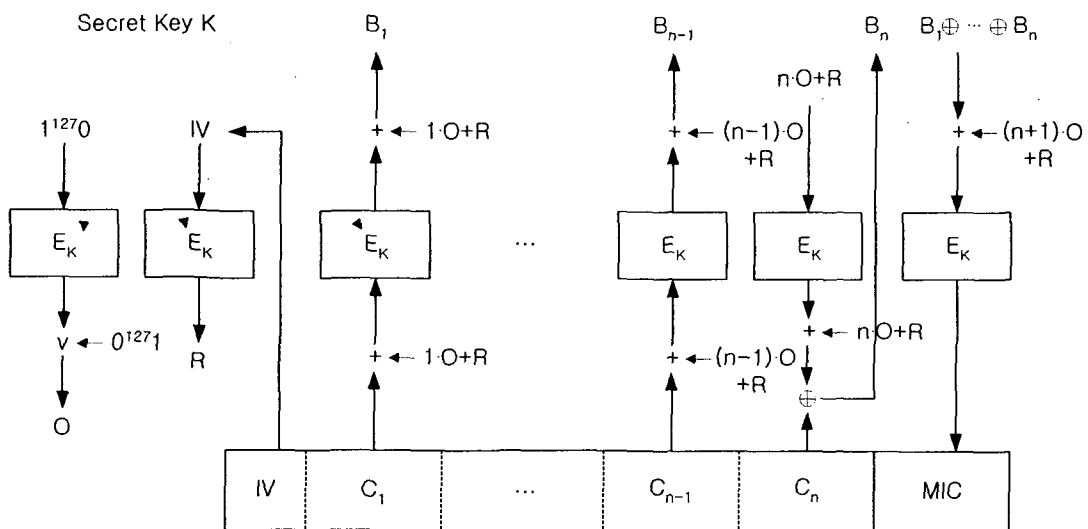


그림 7. AES decipherment block diagram.

$$AES_Encrypt_K(R + n \cdot O) \quad (9)$$

$$B_n = C_i \oplus Mask_{mn}(R + n \cdot O + AES_Encrypt_K(R + n \cdot O)) \quad (10)$$

메시지 무결성은 복호된 데이터로부터 계산된 MIC와 전송된 값을 검사함으로써 이루어진다. 그림 8은 AES 알고리즘을 사용시 WEP에서 구성된 MPDU를 나타낸 것이다.

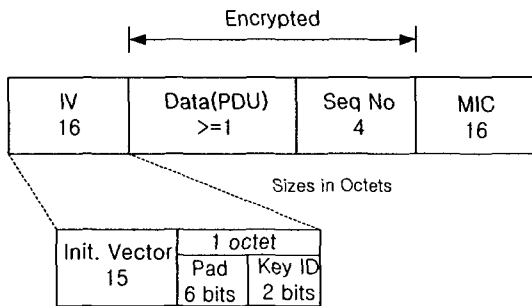


그림 8. Construction of expanded AES MPDU.

AES 알고리즘은 키발생, 암호화 및 복호화 과정으로 구성된다. 키발생 과정은 특별한 링크간 통신 시 적용되며 multicast 및 broadcast 키는 키발생 과정 없이 직접 사용한다. 키는 PMAC 알고리즘을 사용하여 발생되며 PMAC 알고리즘은 OCB 모드와 유사한 MAC 알고리즘에 기초한 블록 암호화 방식이다. 그림 9는 PMAC 과정을 나타낸 것이다. PMAC offset O는 식 (11)과 같이 계산된다.

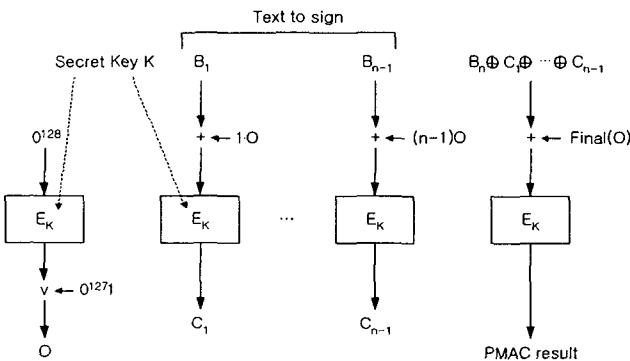


그림 9. PMAC block diagram.

$$O = AES_Encrypt_K(0^{128}) \vee 0^{127}1 \quad (11)$$

각 데이터는 128 비트의 n개 블록으로 분리되며 각 블록은 식 (12)와 같이 암호화 된다.

$$C_i = AES_Encrypt_K(B_i + i \cdot O) \quad (12)$$

마지막 블록이 128 비트인 경우 PMAC 결과는 식 (13)과 같이 계산되며 128 비트보다 작은 경우 PMAC 결과는 식 (14)와 같이 계산된다.

$$PMAC\ result = AES_Encrypt_K((C_1 \oplus \dots \oplus C_{n-1} \oplus B_n) \cdot + Final(O)) \quad (13)$$

$$PMAC\ result = AES_Encrypt_K((C_1 \oplus \dots \oplus C_{n-1} \oplus Pad(B_n)) \quad (14)$$

여기서, Final(O)는 offset O의 비트별 보수이며 Pad(Bn) = 0^{n-m-1}1Bn 이다.

AES 캡슐화 알고리즘은 unicast와 multicast/broadcast 경우 일부 다르다. Unicast인 경우 각 IEEE 802.11 WEP 구현은 AES 알고리즘을 사용한 각 연결에 대하여 암호키와 32비트 순서번호를 유지한다. 암호키는 연결을 형성하는데 사용된 키와 재연결 메시지로부터 유도되며 순서번호는 연결 설정시 0으로 초기화된다. OCB offset O는 키가 발생시 계산되며 IV는 의사 잡음적으로 발생된다.

Multicast/broadcast인 경우 ESS당 하나의 키가 사용되며 순서번호는 사용되지 않는다. AES가 multicast 암호화에 사용될 때 unicast 경우와 같이 OCB offset과 IV를 발생한다.

데이터를 암호화하기 위하여 송신측에서는 데이터 프레임이 unicast인지 혹은 multicast/broadcast인지를 검사한다. 만약, unicast 데이터이면 연결상태를 두고 순서번호를 1씩 증가시킨다. 순서번호가 최대값인 2^{32}-1에 도달하면 재연결을 수행한다. multicast/broadcast 데이터이면 순서번호 영역을 부가하지 않고 multicast/broadcast 상태만 사용된다.

수신측에서 multicast/broadcast 상태는 복호키와 OCB offset을 가지며 unicast 상태는 재사용 윈도우를 부가적으로 포함한다. 재사용 윈도우는 재사용 방지 기능을 제공하고 32 비트 카운트와 64 비트 마스크로 구성되며 0으로 초기화된다. Unicast 데이터가 수신되면 수신측에서는 재사용을 막기 위하여 순서번호를 검사한다. 64 비트 마스크는 최근 수신된 패킷을 기록하는 sliding window이다.

Unicast 패킷이 수신되면 패킷의 순서번호는 저장된 순서번호 및 비트 마스크와 비교된다. 만약, 수신된 순서번호가 저장된 순서번호보다 크다면 과거 순서번호는 수신 순서번호로 대체되고 현재의 수신번호에서 과거의 수신번호를 뺀 차 비트의 비트 마스크를 이동한다. 만약, 수

신된 순서번호가 저장된 순서번호보다 작은 경우 과거의 수신번호에서 현재의 수신번호를 뺀 값이 64 이상이면 너무 오래된 메시지로 간주하고 수신된 패킷을 무시하며 64보다 작다면 해당 비트 마스크가 세트되었는지를 확인한다. 그 비트 마스크가 세트이면 재수신된 메시지로 무시하며 비트 마스크가 세트가 아니면 새로운 메시지로 간주하고 해당 비트 마스크를 세트한다.

V. SMIB

IEEE 802.11 보호 메커니즘은 MAC 관리경로와 관련된 MIB 속성들을 통해 제어된다. 인증이 시도될 때 요구되는 인증 형태는 MLME-AUTHENTICATE.request 프리미티브의 AuthenticationType 파라미터에 의해서 제어된다. STA에 의해서 수용되어질 인증 요구의 형태는 MIB 속성 dot11AuthenticationType에 의해서 제어된다. 인증의 형태는 open system과 shared key의 세트로부터 선택된다.

WEP 호출은 많은 MIB 속성뿐 아니라 MLME-AUTHENTICATE.request 프리미티브로 통한 파라미터들에 의해서 제어된다. WEP 키들을 포함한 모든 MIB 속성은 외부적으로 write-only이며 그 내용들은 MAC 관리 SAP들을 경유하여 판독되지 않는다. 불린 변수 dot11PrivacyInvoked는 1로 설정된 프레임 제어 영역의 WEP 부영역과 함께 MPDU들을 전송하는 것으로부터 STA를 막기 위하여 false로 설정된다. 이것은 MPDU 혹은 MMPDU 수신에 영향을 미치지 않는다.

모든 WEP 키들의 디폴트 값은 null이다. WEP 서브필드가 1로 설정된 프레임을 복호한다는 것은 IV를 분해하고, MPDU에 포함된 데이터상의 ICV와 계산된 ICV 값을 검사하는 것을 포함한다. shared key 구성들을 지원하기 위하여, MIB는 dot11WEPDefaultKeys라고 불리는 4개의 요소 벡터를 포함한다. 이 벡터의 각 요소에 대한 디폴트 값은 null이며 요소들은 WEP으로 사용되기 위하여 디폴트 키들을 가진다.

dot11WEPDefaultKeyID의 속성은 정수이다. 이 값이 0, 1, 2, 또는 3의 값으로 설정될 때, 1로 설정된 프레임 제어 영역의 WEP 부영역으로 전송된 MPDU들은 그 프레임이 개별 RA를 가지고 있지 않고 키 매핑이 프레임의 RA에 존재하지 않는다면 dot11WEPDefaultKeys의 1번째, 2번째, 3번째, 또는 4번째 요소를 사용하여 암호화된다. 수신시, 입력 MPDU는 그 프레임이 개별 RA를 가지고 있지 않고 키 매핑이 프레임의 TA를 위해 존재하지 않는다면 수신된 키 ID 필드에 지정된 dot11WEPDefaultKeys의 요소를 사용하여 복호된다. 전송된 키 ID 영역 값은 dot11WEPDefaultKeyID가 프레

임을 암호화하는 것으로 사용되고 1, 2, 또는 3의 값으로 설정될 때를 제외하고 모든 경우 0이다, 이런 경우 전송된 키 ID 영역은 dot11WEPDefaultKeyID의 값을 포함한다.

불린 속성 aExcludeUnencrypted가 True에 설정되었을 때, 0인 프레임 제어 영역의 WEP 부영역과 함께 STA에 의해서 수신된 MPDU들은 MAC 서비스 인터페이스에서 표시되지 않는다. aExcludeUnencrypted가 True에 설정되었을 때, 단지 성공적으로 복호된 MSDU들이 MAC 서비스 인터페이스에 표시된다.

IEEE 802.11은 같은 WEP 키가 모든 STA에서 사용되지 않으며 MIB는 각 RA/TA 쌍에 대하여 각각의 WEP 키를 공유하도록 한다. 키 매핑은 MIB 속성인 dot11WEPKeyMappings에 의해서 지원된다. dot11WEPKeyMappings는 dot11WEPKeyMappingLength에 의해 나타난 엔트리들의 구현이 정의된 최대 수까지 각 MAC 주소에 대하여 0 내지 1 엔트리를 담고 있으며 각 엔트리를 위해 불린 WEPOn과 대응 WEPKey의 두개 영역을 가진다.

BSS 구조에서 STA MAC 주소에 해당하는 dot11WEPKeyMapping 테이블 엔트리에서의 AP WEPOn 값은 만약 개방형 시스템과 다른 인증 형을 사용하여 인증을 성공적으로 시작 및 끝내지 못했다면 STA를 위해 True로 설정되지 않는다. 모든 WEPOn 영역들의 디폴트 값은 false이다. dot11WEPKeyMappings는 WEP이 무선 링크에 적용되기 때문에 RA 혹은 TA 주소들에 의해서 표시된다. 테이블의 엔트리가 특별한 MAC 주소를 위해 존재할 때, dot11WEPKeyMappings 속성의 값들은 dot11WEPDefaultKeyID와 dot11WEPDefaultKeys 변수들 대신에 사용된다. dot11WEPKeyMappingLength의 최소 값은 10이며 이 값은 WEP 옵션을 구현한 STA를 위한 최소 값을 나타낸 것이다.

데이터 프레임의 전송시 MAUNITDATA.request 프리미티브의 MAC에 의한 수신과 프레임의 전송시간 사이에 지정하지 않은 시간에 dot11PrivacyInvoked, dot11WEPKeyMappings, dot11WEPDefaultKeys, 그리고 dot11WEPDefaultKeyID의 값들은 다음 판단 트리에 따라 사용된다.

```

if dot11PrivacyInvoked is "false"
the MPDU is transmitted without encryption
else
if(the MPDU has an individual RA and
there is an entry in dot11WEPEKeyMappings for that RA)
if that entry has WEPOn set to "false"
the MPDU is transmitted without encryption
else
if that entry contains a key that is null
discard the entire MSDU and generate an
MA-UNITDATA-STATUS.indication primitive to
notify LLC that the MSDU was undeliverable due to
a null WEP key
else
encrypt the MPDU using that entry's key, setting the keyID
subfield of the IV field to zero
else
if(the MPDU has a group RA and the Privacy subfield
of the Capability Information field in this BSS is set to 0)
the MPDU is transmitted without encryption
else
if dot11WEPEDefaultKeys[dot11WEPEDefaultKeyID] is null
discard the msdu and generate an
MA-UNITDATA-STATUS.indication primitive to
notify LLC that the entire MSDU was undeliverable
due to a null WEP key
else
encrypt the MPDU using
dot11WEPEDefaultKeys[dot11WEPEDefaultKeyID],
setting the KeyID subfield of the IV field to
dot11WEPEDefaultKeyID
    
```

데이터 프레임의 수신시 dot11PrivacyOptionImplemented, dot11WEPEKeyMappings, dot11WEPEDefaultKeys, dot11WEPEDefaultKeyID, 그리고 aExcludeUnencrypted 값들은 다음 판단 트리에 따라 사용된다.

```

if the WEP subfield of the Frame Control Field is zero
if a ExcludeUnencrypted is "true"
discard the frame body without indication to LLC and increment
dot11WEPEExcludedCount
else
receive the frame without decryption
else
if dot11PrivacyOptionImplemented is "true"
if(the MPDU has individual RA and
there is an entry in dot11WEPEKeyMappings matching the MPDU's TA)
if that entry has WEPOn set to "false"
discard the frame body and increment
dot11WEPEUndecryptableCount
else
if that entry contains a key that is null
discard the frame body and increment
dot11WEPEUndecryptableCount
else
attempt to decrypt with that key, incrementing
dot11WEPEICVErrorCount if the ICV check fails
else
if dot11WEPEDefaultKeys[keyID] is null
discard the frame body and increment
dot11WEPEUndecryptableCount
else
attempt to decrypt with dot11WEPEDefaultKeys[keyID],
incrementing dot11WEPEICVErrorCount if the ICV check fails
else
discard the frame body and increment dot11WEPEUndecryptableCount
    
```

관리 프레임을 전송시, ATSN(authentication transaction sequence number) 영역 값이 2일때 MAC는 다음 판단 트리에 따라 동작한다.

```

if dot11PrivacyOptionImplemented is "false"
the MMPDU is transmitted with a sequence
of zero octets in the Challenge Text field and a Status Code value of 13
else
the MMPDU is transmitted with a sequence of 128 octets generated using
the WEP PRNG and a key whose value is unspecified and beyond the
scope of this standard and a randomly chosen IV value (note that this
will typically be selected by the same mechanism for choosing IV values
for transmitted data MPDUs) in the Challenge Text field and a status
code value of 0 (the IV used is immaterial and is not transmitted).
Note that there are cryptographic issues involved in the choice of
key/IV for this process as the challenge text is sent unencrypted and
therefore provides a known output sequence from the PRNG.
    
```

관리 프레임을 수신시, ATSN 영역 값이 2일때 MAC는 다음 판단 트리에 따라 동작한다.

```

if the WEP subfield of the Frame Control field is 1
respond with a status code value of 15
else
if dot11PrivacyOptionImplemented is "true"
if there is a mapping in dot11WEPEKeyMappings matching the MSDU's TA
if that key is null
respond with a frame whose Authentication Transaction
Sequence Number field is 3 that contains the appropriate
Authentication Algorithm Number, a status code value of
15 and no Challenge Text field, without encrypting the
contents of the frame
else
respond with a frame whose Authentication Transaction
Sequence Number field is 3 that contains the appropriate
Authentication Algorithm Number, a status code value of
0 and the identical Challenge Text field, encrypted using
that key, and setting the key ID subfield in the IV field to 0
else
if dot11WEPEDefaultKeys[dot11WEPEDefaultKeyID] is null
respond with a frame whose Authentication Transaction
Sequence Number field is 3 that contains the appropriate
Authentication Algorithm Number, a status code value of
15 and no Challenge Text field, without encrypting the
contents of the frame
else
respond with a frame whose Authentication Transaction
Sequence Number field is 3 that contains the appropriate
Authentication Algorithm Number, a status code value of 0
and the identical Challenge Text field, encrypted using
dot11WEPEDefaultKeys[dot11WEPEDefaultKeyID], setting the
key ID subfield in the IV field to dot11WEPEDefaultKeyID
else
respond with a frame whose Authentication Transaction
Sequence Number field is 3 that contains the appropriate Authentication
Algorithm Number, a status code value of 13 and no Challenge Text
field, without encrypting the contents of the frame
    
```

관리 프레임을 수신시, ATSN 영역 값이 2일때 MAC는 다음 판단 트리에 따라 동작한다.


```

if the WEP subfield of the Frame Control field is zero
  respond with a status code value of 15
else
  if dot11PrivacyOptionImplemented is "true"
    if there is a mapping in dot11WEPKeyMappings matching the MSDU's TA
      if that key is null
        respond with a frame whose Authentication Transaction
          Sequence Number field is 4 that contains the appropriate
          Authentication Algorithm Number, and a status code value
          of 15 without encrypting the contents of the frame
      else
        attempt to decrypt with that key, incrementing
          dot11WEPCVErrorCount and responding with a status code value
          of 15 if the ICV check fails
    else
      if dot11WEPDefaultKeys[keyID] is null
        respond with a frame whose Authentication Transaction
          Sequence Number field is 4 that contains the appropriate
          Authentication Algorithm Number, and a status code value
          of 15 without encrypting the contents of the frame
      else
        attempt to decrypt with dot11WEPDefaultKeys[keyID],
          incrementing dot11WEPCVErrorCount and responding with
          a status code value of 15 if the ICV check fails
    else
      respond with a frame whose Authentication Transaction Sequence Number
        field is 4 that contains the appropriate Authentication Algorithm Number,
        and a status code value of 15
    
```

기술,” 한국정보보호학회지, vol. 12, no. 1, pp.66-74, 2002년 2월

- [3] ISO/IEC 8802-11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.
- [4] IEEE 802.11b, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Higher- speed Physical Layer Extension in the 2.4 GHz Band*, 1999.
- [5] IEEE 802.11a, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : High- speed Physical Layer in the 5 GHz Band*, 1999.
- [6] IEEE 802.11eS/D1, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Specification for Enhanced Security*, March 2001.

VI. 결 론

무선 LAN은 다양한 정보와 자원을 공유할 수 있게 하는 LAN의 장점과 제약 없는 연결성 제공이라는 편리성을 동시에 제공하는 무선통신 기술의 결정체로 각광을 받고 있으나 전파라는 무선매체를 사용함으로써 정보도용의 가능성이 높으며 감시도 어렵다는 특징을 가지므로 정보보호기술이 문제점으로 대두되고 있다. 본 연구에서는 무선 LAN에서의 핵심 정보보호기술인 ESN, WEP, AES 및 SMIB에 관하여 기술하였다. IEEE 802.11 표준안에서 사용한 WEP 방식은 사용된 키와 IV 값이 작아서 암호학적인 정교한 공격에는 보호를 제공할 수 없고 데이터 변형 및 재사용을 막을 수 없으므로 128비트 암호화 키와 IV를 사용하도록 IEEE 802.11eS 초안에서 제시하였다. 또한, IEEE 802.11eS 초안에서는 무선 LAN에서의 인증과 키 관리 서비스를 제공하기 위하여 MAC 계층 위에 ESN 프로토콜을 적용하였으며 AES 알고리즘을 제시하였다.

참 고 문 헌

- [1] 정의석, 조용수, “IEEE 802.11a 고속 LAN 모뎀 기술,” 한국통신학회지, vol. 16, no. 10, pp.42-63, 1999 10월
- [2] 박영호, 김철수, 윤정오, “무선 LAN에서의 정보보호