무선 LAN을 위한 보호시스템에 관한 연구†
(A study on the security system for wireless LAN)

박 영 호*, 김 철 수**
(Young-Ho Park , Cheol-Su Kim)

요 약 무선 LAN은 무선통신 기술의 결정체로 각광을 받고 있으나 전파라는 무선매체를 사용함으로써 정보도용의 가능성이 높으며 감시도 어렵다는 특징을 가지므로 정보보호가 요구된다. 본 논문에서는 무선 LAN을 위한 보호시스템을 제시하기 위하여 IEEE 802.11 표준안 및 IEEE 802.11eS 초안에서 제시하는 무선 LAN의 보호모델과 WEP 및 AES 암/복호화 방식에 관하여 정의하고 이러한 방식에 적합한 키분배 프로토콜을 제안한다.

Abstract The rapid progress of wireless LAN technology has prompted new security problems and countermeasures against them. Since the mobility of users and wireless access to the network exasperate potential security threat such as eavesdropping and illegal access, security services for wireless LAN should be provided. In this paper, we define the security model, WEP and AES encrypt/decrypt technologies which are proposed in the IEEE802.11 standard and the IEEE802.11eS draft and propose the Key distribution protocol for the wireless LAN.

1. 서 론

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.[1-3] 무선 LAN에 대한 국제 표준화는 1990년 10월부터 IEEE 802.11 위원회에 의해 무선 매체 접근 제어(medium access control)와 물리 계층 규격에 대한 표준화가 OSI 참조 모델에 준하여 진행되고 있으며 무선 멀티미디어 서비스 요구의 증가와 무선 전송기술의 발달로 인하여 1~2 Mbps 전송속도를 갖는 무선 LAN의 표준안인 IEEE 802.11[4] 규격을 향상시켜 2.4GHz 대에서 1~11 Mbps의 전송속도를 갖는 IEEE 802.11b 표준안[5]을 5 GHz 대에서 6~54 Mbps의 전송속도를 갖는 IEEE 802.11a 표준안[6]을 제시하였다.

무선 LAN 서비스는 전파라는 무선매체를 사용함으로써 이동성, 휴대성 등의 편리성을 제공하는 반면 정보도용의 가능성이 높으며 감시도 어렵다는 특징을 가지므로 정보보호가 요구된다. IEEE 802.11 표준안에서는 무선 LAN에서의 정보를 보호하기 위하여 WEP(wired equivalent privacy) 방식을 사용하였다. WEP에서는 IV(initialization vector)를 변경함으로써 발생되는 키를 사용하므로 brute-force에 의한 비밀키 획득이 어려우며 각 메시지에 대하여 self-synchronizing 하며 하드웨어 및 소프트웨어적으로 구현이 쉽다는 장점이 있다. 또한, WEP은 평문이 동일한 길이의 의사잡음 키열과 비트별 XOR 연산을 수행함으로써 암호문을 발생한다. IEEE 802.11eS 초안[7]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

† 이 논문은 2002년 상주대학교 학술연구비지원에 의해 연구되었음.
* 상주대학교 전자전기공학과 부교수 (yhpark@sangju.ac.kr)
** 경주대학교 컴퓨터전자공학부 조교수

스트림을 암호화함으로써 데이터 보호를 MIC(message integrity code)를 계산함으로써 데이터 무결성을 제공하는 효율적인 방식이다.

암호화 방법에는 크게 대칭 키 암호화 방법 및 비대칭 키 암호화 방법이 있다. 대칭 키 암호화 방법은 처리속도가 빠르고 구현이 간단하나 키 관리가 문제된다. 비대칭 키 암호화 방법은 처리속도가 상대적으로 느리지만 키 관리 및 인증의 기능을 효과적으로 수행할 수 있다. 따라서 일반적으로 정보보호를 위한 암호화 시스템의 구현에서 키 분배에는 비대칭 암호화 방법을 이용하고 이 분배된 암호화 키를 사용하여 전송 데이타의 암복호에는 대칭 키 암호화 방법을 이용한다.[8-9]

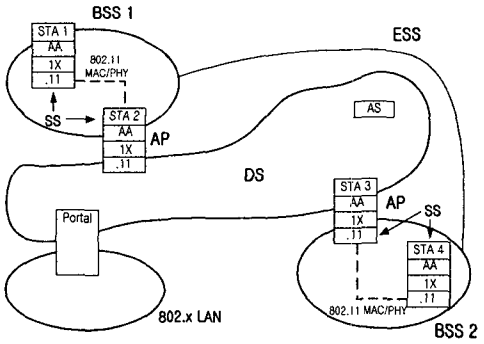
본 논문에서는 무선 LAN을 위한 보호시스템을 제시하기 위하여 IEEE 802.11 표준안 및 IEEE 802.11eS 초안에서 제시하는 무선 LAN의 보호모델과 WEP 및 AES 암/복호화 방식에 관하여 정의하고 이러한 방식에 적합한 키분배 프로토콜을 제안한다. 제안한 키분배 프로토콜에서는 identity를 사용함으로써 상호 신분 인증 기능을 가지며 전송하는 데이타의 인증을 위하여 해쉬와 암호화를 결합한 방식을 사용한다. 본 논문의 구성은 다음과 같다. 2장에서는 IEEE 802.11 무선 LAN의 일반적인 구조 및 서비스에 관하여 기술하고 3장에서는 IEEE 802.11 표준안의 WEP에 IEEE 802.11eS draft에서 제시한 기능을 부가하여 WEP을 기술하며 4장에서는 AES 알고리즘의 동작을 기술하고 5장에서는 무선 LAN에 적합한 키분배 프로토콜을 기술한다. 마지막으로 6장에서는 결론을 맺는다.

2. 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 구조블록으로 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. Portal는 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 메카니즘은 ULAP에 의존한다.

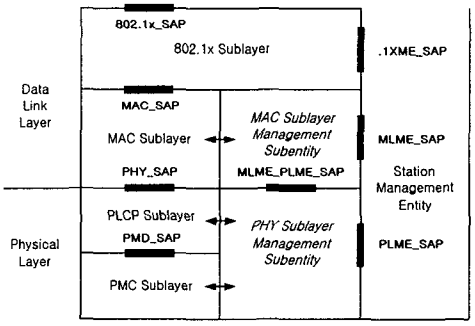
IEEE 802.11에서 제공하는 서비스들은 연결, 해제, 분배, 통합, 재연결, 인증, deauthentication, 데이터 인증, 키 분배, 프라이버시, 재사용 방지 그리고 MSDU 전달이다. 이 서비스들은 STA에서의 서비스와 DS에서의 서비스로 분류된다. STA에서 제공되는 서비스들은 인증, 데이터 인증, deauthentication, 키 분배, 프라이버시, 재사용 방지 및 MSDU 전달이며 DS에서 제공되는 서비스들은 연결, 해제, 분배, 통합 및 재연결 이다. 이 12개의 서비스들 중 연결, 해제, 분배, 통합, 재연결 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 메체로 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 링크 레벨 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.



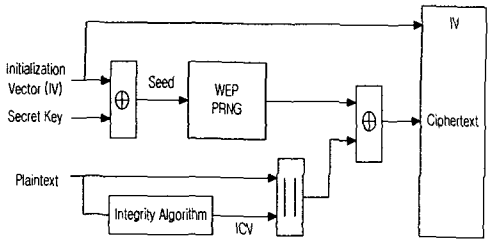
<그림 2> Portion of the ISO/IEC reference model covered in IEEE 802.11.

3. WEP

IEEE 802.11은 무선 LAN에서의 인가된 사용자를 보호하기 위하여 WEP 방식을 사용하고 있다. WEP에서는 초기벡터 IV를 변경함으로써 발생되는 키를 사용하므로 brute- force 에 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

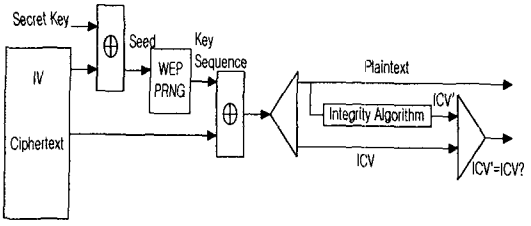
PRNG(pseudo random number generator)에 입력된다. 비밀키와 IV는 128 비트이며 비밀키가 128 비트보다 작은 경우 나머지 영역은 0으로 채워지며 128 비트보다 큰 경우는 잘라낸다. PRNG의 출력은 데이터 octet의 길이와 같은 의사잡음 octet의 키열이다. 비인가된 데이터 변경을 막기 위하여 무결성 알고리즘을 평문에 적용하여 4 octets의 ICV 값을 발생한다. 암호화는 발생된 키열과 평문 및 ICV 값을 XOR 연산을 함으로써 이루어지며 암호화 과정의 출력값은 IV와 암호문이다. WEP PRNG는 비교적 짧은 길이의 비밀키를 입력하여 비교적 긴 키열을 발생하는 암호화과정의 중요한 요소이다. IV는 비밀키의 수명을 연장시키고 알고리즘의 자기동기성질을 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.



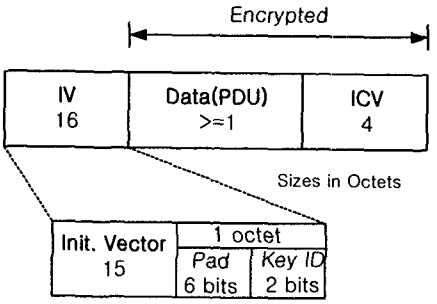
<그림 3> WEP encipherment block diagram.

그림 4는 WEP 복호화 과정을 나타낸 것이다. 수신 메시지의 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 5는 WEP 알고리즘에 의해 구성된 암호화된 프레임을 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.



<그림 4> WEP decipherment block diagram.



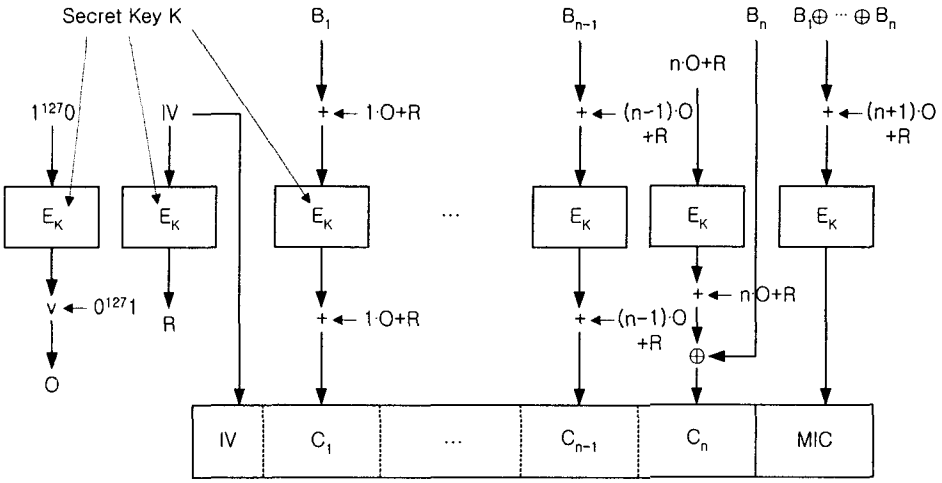
<그림 5> WEP frame.

4. 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 데이터 무결성을 제공하는 효율적인 방식이다. OCB 모드는 n 블록의 데이터를 암호화하고 MIC를 부가하는데 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.

$$O = AES\_EncryptK(1^{127}0) \vee 0^{127}1 \qquad (1)$$

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.



<그림 6> AES encipherment block diagram.

$$R = AES\_EncryptK(IV) \quad (2)$$

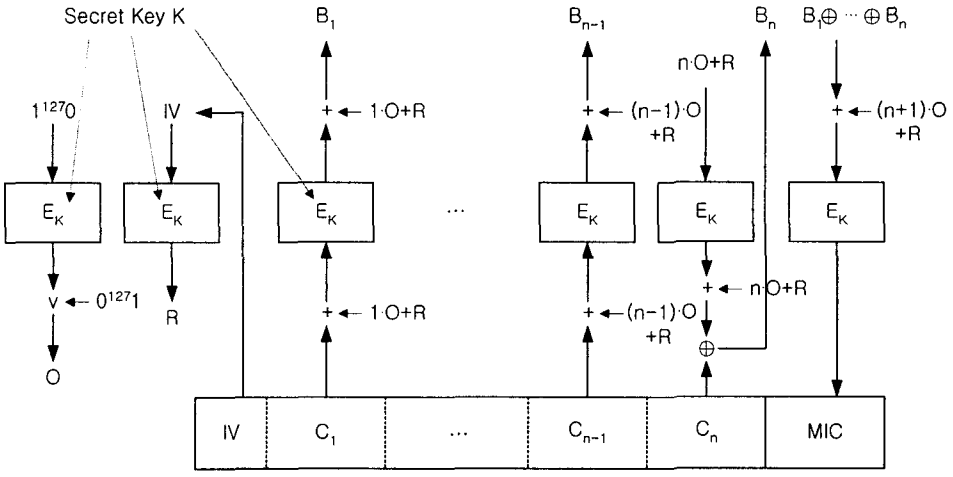
R과 offset O는 암호화 전후과정에서 사용된다. OCB 모드 암호화는 데이터를 128비트 블록으로 분리하며 i= 1 .. n-1 번째까지의 블록 데이터는 식 (3)과 같이 암호화된다.

$$C_i = R + i \cdot O + AES\_Encrypt_K (R + i \cdot O + Bi) \quad (3)$$

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

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

$$C_n = B_n \oplus Mask_{m,n}(R + n \cdot O + AES\_Encrypt_K(R + n \cdot O)) \quad (5)$$



<그림 7> AES decipherment block diagram.

식 (5)에서 $Mask_{m,n}(A)$는 A의 m+1에서 n번째 까지의 비트를 마스크 한다는 것을 의미하며 ⊕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.

$$MIC = AES\_Encrypt_K((B_1 \oplus B_2 \oplus \cdots B_n) + R + (n+1)\cdot O) \quad (6)$$

$$MIC = AES\_EncryptK((B1 \oplus B2 \oplus \cdots B_{n-1} \oplus Pad_{m,n}(B_n)) + R + (n+1)\cdot O) + R + (n+2)\cdot O) \quad (7)$$

식 (7)에서 $Pad_{m,n}(A) = 0^{n-m-1}1A$ 이다. 그림 7은 AES 복호화 블록 다이어그램을 나타낸 것이다.

각 블록 B_i는 식 (8)과 같이 복호된다.

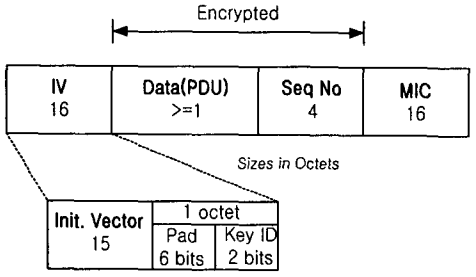
$$B_i = AES\_Decrypt_K(C_i - (R+i\cdot O)) - (R+i\cdot O) \quad (8)$$

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

$$B_n = B_n \oplus (R + n\cdot O + AES\_Encrypt_K(R + n\cdot O)) \quad (9)$$

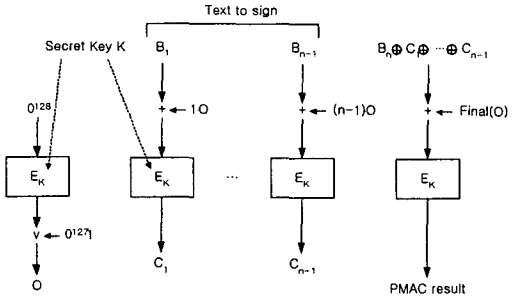
$$B_n = C_i \oplus Mask_{m,n}(R + n\cdot O + AES\_Encrypt_K(R + n\cdot O)) \quad (10)$$

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.

$$PMAC\ result = AES\_Encrypt_K((C1 \oplus \cdots \oplus C_{n-1} \oplus B_n) + Final(O)) \quad (13)$$

$$PMAC\ result = AES\_Encrypt_K((C_1 \oplus \cdots \oplus C_{n-1} \oplus Pad(B_n)) \quad (14)$$

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

AES 캡슐화 알고리즘은 *unicast*와 *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.

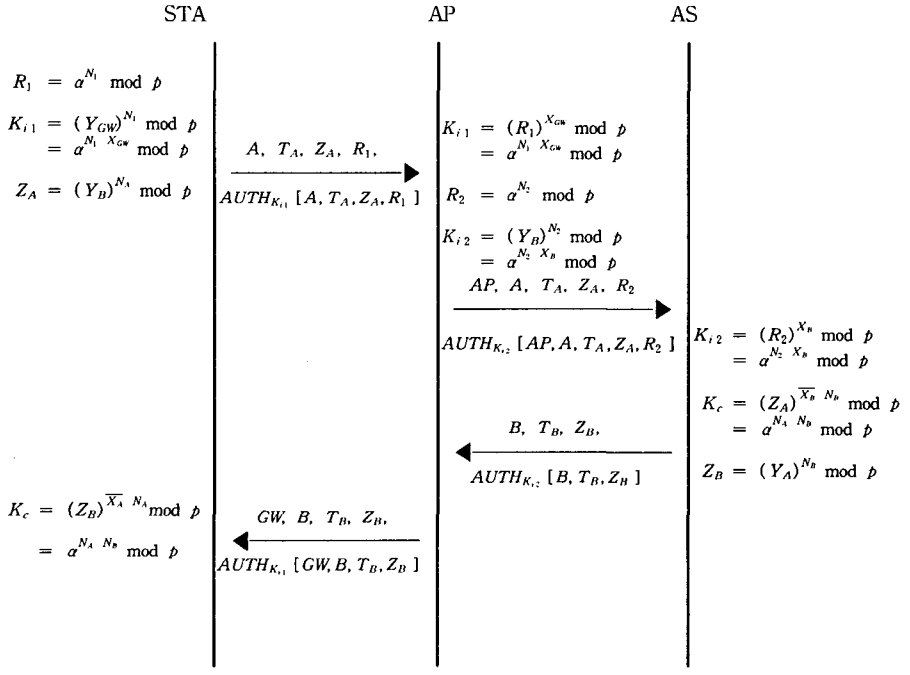
Multicat/broadcast인 경우 ESS당 하나의 키가 사용

되며 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 $2^{32}-1$에 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 대치되고 현재의 수신번호에서 과거의 수신번호를 뺀 차 비트의 비트 마스크를 이동한다. 만약, 수신된 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.



where, AP : Access Point, AS : Authentication Server
K_{i1}, K_{i2} : Integrity key, K_c : Confidentiality key,
T_A, T_B : Time stamp,
N_A, N_B, N_1, N_2 : Random number,
$AUTH_{K_{i1}}[A, T_A, V_A, R_1] = E_{K_{i1}}[FHASH(A, T_A, V_A, R_1)]$

<그림 10> The key distribution protocol with an authentication function in the wireless LAN.

5. 키 분배 프로토콜

무선 LAN에서 보호 서비스를 효율적으로 제공하기 위하여 중간 시스템인 AP에서는 무결성 서비스를 종단 시스템인 STA와 AS 간에는 무결성 및 비밀보장 서비스의 제공이 필요하다. 이러한 보호 서비스를 제공하기 위해서는 안전하고 효율적인 키 분배가 필요하다. 따라서 본 논문에서는 무선 LAN을 위한 키 분배 프로토콜을 그림 10과 같이 제안한다.

본 키 분배 프로토콜에서는 무결성을 위한 키를 분배하기 위하여 일방 간접 인증 기능을 갖는 one-pass 메카니즘인 ElGamal 방식[9,10]을 이용하며 비밀보장을 위한 키를 분배하기 위하여 D-H형 방식[11]을 이용한다. 본 프로토콜은 identity를 사용함으로써 상호 신분 인증 기능을 가지며 전송하는 데이타의 인증을 위하여 해쉬와 암호화를 결합한 방식을 사용한다. 또한, 본 프로토콜은 메세지의 컴팩트, 다른 네트워크에 대한 융통성 그리고 보안도도 높다.

제안한 키 분배 프로토콜의 절차는 다음과 같다.

① STA는 랜덤 수 N_I, N_A와 time stamp T_A를 발생하고 무결성 검사 키 발생에 사용될 R_I, 무결성 검사 키 K_{i1}, 비밀보장 키 발생에 사용할 Z_A를 계산한다. STA의 상태값, T_A, Z_A, R_I 그리고 인증값을 AP에 전송한다. 인증값인 $AUTH_{K_{i1}}[A, T_A, Z_A, R_I]$는 $E_{K_{i1}}[FHASH[A, T_A, Z_A, R_I]]$이다. 여기서, FHASH[ ]는 단방향 해쉬함수이며 $E_{K_{i1}}[]$는 키 K_{i1}에 의한 암호화 함수이다.

② AP는 전송된 R_I과 자신의 비밀키를 사용하여 무결성 검사 키 K_{i1}를 구한후 인증값을 검증한다. 인증값이 맞으면 AS와 사용될 무결성 검사 키를 발생하기 위하여 랜덤수 N_2를 발생하고 무결성 검사 Z_A 키 발생에 사용될 R_2 및 무결성 검사 키 K_{i2}를 계산한다. 중간 시스템의 상태값 AP, T_A, R_2 그리고 인증값을 AS에게 전송한다.

③ AS는 T_A를 검사하여 최종 도착지까지 허용시간 내에 데이타의 도착 여부를 확인하고 무결성 검사 키 K_{i2}를 구한 후 수신된 인증값을 검증한다. AS는 수신된 Z_A를 이용하여 비밀보장에 사용할 키 Z_c를 구하고 자신의 상태값 B, time stamp T_B, 비밀보장 키 발생에 사용할 Z_B 그리고 인증값을 중간 시스템에게 전송한다.

④ AP는 무결성 검사 키 K_{i2}를 이용하여 수신된 인증값을 검증한 후 자신의 상태값을 STA에게 전송한다.

⑤ STA는 T_B를 검사하여 최종 도착지까지 허용시간 내에 데이타의 도착 여부를 확인한 후 K_{i1}를 이용하여 수신된 인증값을 검증한다. 수신된 Z_B를 이용하여 비밀보장에 사용할 키 K_c를 구한다.

6. 결론

본 논문에서는 무선 LAN을 위한 보호시스템을 제시하기 위하여 IEEE 802.11 표준안 및 IEEE 802.11eS 초안에서 제시하는 무선 LAN의 보호모델과 WEP 및 AES 암/복호화 방식에 관하여 정의하였고 이러한 방식에 적합한 키분배 프로토콜을 제안하였다. 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. 제안한 키분배 프로토콜은 무선 LAN에서 identity를 사용함으로써 상호 신분 인증 기능을 가지며 전송하는 데이타의 인증을 위하여 해쉬와 암호화를 결합한 방식을 사용하였다. 또한, 본 프로토콜은 메세지의 컴팩트, 다른 네트워크에 대한 융통성 그리고 보안도도 높다. 무선 LAN 상에서 그룹 키 관리 등이 추후 연구과제이다.

참 고 문 헌

[1] 박영호,김철수,윤정오,"무선 LAN에서의 정보보호기술," 정보보호학회지, Vol.12, No.1, pp. 66-74, 2002년 2월

[2] 신영환, 박영호, "무선 LAN 보호를 위한 IEEE 802.11 표준안에 관한 연구," 한국산업정보학회 춘계학술대회논문집, pp.80-88, 2002년 6월

[3] 정의석, 조용수, "IEEE 802.11a 고속 LAN 모뎀 기술," 한국통신학회지, 16(10), pp.42-63, October 1999.

[4] ISO/IEC 8802-11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.

[5] 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.

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

[7] IEEE 802.11eS/D1, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Specification for Enhanced Security*, March 2001.

[8] Y. H. Park and S. J. Moon "Protection boundary for internetwork security," *IEE Electronics Letters*, vol. 31, no. 10, pp.776-778, May 1995.

[9] ISO/IEC, *Key Management Part 3 : Key Management using Asymmetric Cryptographic Techniques*, CD 11770-3, July 1993.

[10] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. on Information Theory*, vol. IT-31, no. 4, pp.469-472, July 1985.

[11] T. Matsumoto, Y. Takashima, and H. Imai "On seeking smart public-key distribution systems," *IEICE Trans.*, vol. E69, no. 2, pp.99-106, February 1986.

박 영 호 (Young-Ho Park)

1989년 경북대학교 전자공학과(공학사)
1991년 경북대학교 대학원 전자공학과 (공학석사)
1995년 경북대학교 대학원 전자공학과 (공학박사)
1996년 3월 ~ 현재 : 상주대학교 전자전기공학부 부교수
관심분야 : 정보보호, 이동통신 등

김 철 수 (Cheol-Su Kim)

1989년 경북대학교 전자공학과(공학사)
1991년 경북대학교 대학원 전자공학과 (공학석사)
1997년 경북대학교 대학원 전자공학과 (공학박사)
1995년 3월~1998년 2월 김천대학 전자통신과
1998년 3월 ~ 현재 : 경주대학교 컴퓨터전자공학부 조교수
관심분야 : 광통신, 정보보호 등