IEEE 802.11i의 상호인증과 키 생성 및 교환 메커니즘 분석

박지혜, 문일현, 이옥연, 김창범

국민대학교, 수학과

Analysis of Mutual Authentication, Key generation and Key exchange mechanism of IEEE 802.11i

Jee-Hye Park, Il-Hyoen Moon, Okyeon Yi, Chang Bum Kim

Department of Mathematics, Kookmin Univ.

snoopy1@kebi.com , cryptology@hitel.net , {oyyi, cbkim}@kookmin.ac.kr

요 약

기존의 무선 랜의 보안상의 문제점들을 해결하기 위하여 사용자와 인증자사이의 상호인증과 키를 교환하는 메커니즘이 요구된다. 이것을 보안하기 위해 IEEE 802.11i에서 키 체계와 4-Way Handshake를 제안하였다. 본 논문에서 언급되는 키 생성 및 교환 메커니즘은 사용자와 서버간의 인증된 마스터 키를 통한 사용자와 인증자의 상호인증과, 키 생성과 키 교환하는 방법에 초점을 맞추고 있다. 이러한 키를 생성하기 위한 Pairwise 키 체계와 키 교환을 위한 4-Way Handshake, 4-Way Handshake에서 사용되는 EAPOL-Key message에 대하여 분석하였다.

I. 서론

무선 랜이란 무선매체를 통해 데이터를 전달하는 기존의 유선 랜이 제공하는 서비스를 제공하는 기술이다. 무선 랜의 이점으로는 유선 랜과는 다르게 이동할 수 있다는 이동성과 케이블링을 할 필요가 없으므로 구축의 유연성, 비용절감과 확장성이 있다. 그러나 기존의 무선 랜에는 다음과 같은 문제점이 존재한다. 먼저 AP와 STA간의 상호인증을 지원하지 않고 AP가 일방적으로 STA만을 인증한다. 또한 802.11b에서 사용중인 WEP이 동적인 WEP 키를 지원하지 않기 때문에 한 번 인증되면 계속 같은 키를 사용해야하는 알고리즘내의 키 스케줄링 문제가 생긴다. 기존 무선 랜의 이런 문제를 해결하고자 IEEE에서는 다음과 같은 해결방안을 제시하였다.

IEEE에서 진행 중인 802.11i draft 4.0 [2]에서는 802.1x[3] 포트기반을 통한 STA와 AP간의 상호인증과 키 분배 및 고정적인 키 문제를 4-Way Handshake와 Group Key Handshake로 해결함으로써 무선구간에서의 보안 문제를 해결하고자 한다.

본 논문에서는 IEEE 802.11i draft 4.0에서 제시하는 상호인증, Pairwise Key 및 Group Key 생성을 위한 키 체계와 키 교환 메커니즘인 4-Way Handshake에 대해 자세히 분석한다.

II. 본문

1. Pairwise key hierarchy

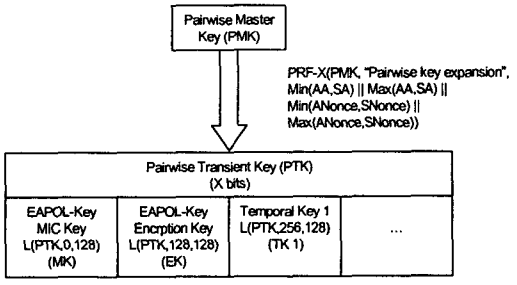

그림 1 Pairwise key hierarchy

Pairwise key hierarchy는 그림 1에서 명시되어 있는 것처럼 PMK (Pairwise Master Key : 256

bits)로부터 특수한 세션키를 획득하기위해 PRF-384 또는 PRF-512를 활용한다. Pairwise key hierarchy는 PMK로부터 PTK (Pairwise Transient Key)를 생성한다. PTK는 EAPOL-Key MIC Key, Encryption Key, Temporal Key로 구분되며 Pairwise Key는 한 쌍의 요청자와 인증자 사이에서 사용된다.

각 매개변수에 대해서는 다음 표에서 설명한다.

SNonce	요청자에 의해 제공되는 난수 또는 의사난수
ANonce	인증자에 의해 제공되는 난수 또는 의사난수
PTK	PRF에의해 PMK로부터 유도 PTK ← PRF-X(PMK, "Pairwise key expansion", Min(AA,SA) || Max(AA, SA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))
MK	PTK의 0-127비트 MK ← L(PTK, 0, 128) 1)
EK	PTK의 128-255비트 EK ← L(PTK, 128, 128)
TK1	PTK의 256-383비트 TK1 ← L(PTK, 256, 128)
TK2 (option)	PTK의 384-511비트 TK2 ← L(PTK, 384, 128) • TKIP 사용 시 생성

표 1 Pairwise 키 체계의 매개변수

2. EAPOL Key Message

IEEE 802.11에서 암호화키와 STA와 인증자간의 정보를 교환하기위해 EAPOL-Key Message를 사용한다. EAPOL Key Message format은 그림 2에서 보여준다.

• Descriptor Type : RSNA Key Descriptor를 확인하기 위한 1 octet 길이로서 254값을 갖는다.

• Key Information : 크기는 2 octet이고 키의 특성을 지정한다.

Bit 규칙은 IEEE 802.1x와 같이 사용된다. Key information bit는 표 2 에서 설명한다.

• Key Length : 이 부분은 부호비트 없는 2진수로서 길이가 2octet이며 IEEE 802.11의 설정에 필요한 키의 octet 길이를 정의한다.

• Key Replay Counter : 이 부분은 부호비트 없는 2진수로서 8octet이고 PMK가 설정될 때 0으로 초기화된다. EAPOL-Key message에 응답할 때 요청자는 수신된 EAPOL-Key message의 Replay Counter를 사용한다. 재사용되는 EAPOL-Key message를 방지하기 위해서 사용되는 sequence number를 나타낸다. Replay Counter는 (재)결합에서 0으로 초기화된다. 인증자는 각 EAPOL-Key message마다 Replay Counter를 증가시킨다. 인증자로부터의 메시지에 응답할 때 요청자는 인증자로부터 수신한 Replay Counter를 사용한다. 요청자는 수신된 정당한 메시지보다 작은 Replay Counter를 포함하는 EAPOL-Key Message는 무시한다. 보통 Replay Counter는 EAPOL-Key MIC이 검증된 후 갱신된다.

Descriptor Type 1 octet	
Key Information 2 octet	**Key Length** 2 octet
Replay Counter 8 octet	
Key Nonce 32 octet	
EAPOL-Key IV 16 octet	
Key RSC 8 octet	
Key ID 8 octet	
Key MIC 16 octet	
Key Material Length 2 octet	**Key Data** n octet

그림 2 EAPOL-Key Descriptor

• Key Nonce : 이 부분은 32octet이다. Key Nonce 값은 인증자의 ANonce 또는 GNonce를 전달하고 요청자의 SNonce를 전달한다. Nonce가 불필요한 전송의 경우 0으로 정해진다.

• Key IV : 이 부분은 16octet이다. Group Key를 암호화하는 키와 함께 사용되는 IV를 포함한다. 메시지가 Pairwise Key를 지정하고 있을 때는 0으로 세팅된다.

• Key RSC : 8octet을 차지하며 IEEE 802.11에서 설치되는 키의 수신된 수열번호(receive sequence counter (RSC))를 나타낸다. Replay 상태를 일치시키기 위해 4-Way Handshake의 메시지 3과 그룹키 갱신의 첫 번째 메시지에만 사용된다. 다른 메시지의 경우 0으로 설정된다. Key RSC의 길이가

8octet보다 작은 경우 나머지 octet을 0으로 설정한다.

• Key ID : 길이가 8octet이고 0으로 설정된다.

	설 명
Key Descriptionversion Number(bit 0~2)	Key Descriptor Version Type 지정 · Type 1: HMAC-MD5, RC4 사용 · Type 2: HMAC-SHA1-128, Key wrap사용
Key Type(bit 3)	Pairwise키 또는 Group키 지정 · 1 : Pairwise 키· 2 : Group 키
Key Index(bit 4~5)	메시지로부터 유도된 키에서 얻어진 Temporal Key의 Key id를 지정. 0~3까지 사용
Install flag(bit 6)	Pairwise Key라면· 1 : Temporal Key TK1, TK2를 STA에 설정· 2 : 설정하지 않음
	Group Key라면 · 1 : Temporal Key TK1, TK2를 송수신을 위해 설정· 2 : Temporal Key TK1, TK2를 수신용으로 설정
Key Ack(bit 7)	EAPOL-Key message 응답요구
Key MIC(bit 8)	EAPOL-Key message 안의 MIC유무
Secure(bit 9)	Link를 초기화하기위해 필요한 키값을 모두 받음으로써 연결상태가 안전하다고 판단시 1로 설정
Error(bit 10)	요청자가 MIC실패를 전할시 1로 설정
Request(bit 11)	요청자가 인증자에게 새로운 4-Way Handshake 요청시 1로 설정
Reserved(bit 12~15)	0으로 설정하고 무시한다.

표 2 Key information bit layout

• Key MIC : Key Descriptor Version field가 1 또는 2일 때 이 부분의 길이는 16octet이다. EAPoL-Key MIC은 Key Material field를 암호화하고 EAPoL-Key MIC field를 0으로 설정한 후 EAPOL Protocol Version field부터 EAPOL-Key Material field까지의 EAPOL packet에 대한 MIC 값이다. Key Data field가 Group Key를 포함하는 경우 GTK는 MIC 값이 계산되기 전에 암호화된다.- Key Descriptor Version 1: HMAC-MD5; RFCs 2104와 1321에서 정의.

- Key Descriptor Version 2: HMAC-SHA-1.

• Key Data Length : 부호비트가 없는 2진수를 기술하기 위해 2octet을 사용한다. 이것은 Key Data field의 octet 길이를 나타낸다.

• Key Data : Pairwise Key를 지정한 EAPOL-Key messages에서 4-Way Handshake의 메시지 2와 3의 Key Data field는 RSN IE를 포함하고, 메시지 1과 4는 아무것도 포함하지 않는다.

Group TK의 경우 Key Data field 부분에 암호화된 GTK 값을 설정한다.

- Key Descriptor Version 1: RC4는 유도된 PTK로부터 EK 부분을 사용하는 Key Data field를 암호화하는데 사용된다.

- Key Descriptor Version 2: RFC 3394에 정의된 AES Key Wrap을 이용하여 PTK로부터 유도된 EK로 Key Material field를 암호화한다.

3. EAPOL-Key message notation

다음은 EAPOL-Key Frame의 frame body를 나타낸다. 각 매개변수에 대해 다음 표 4 에서 설명한다.

EAPOL-Key(S, M, A, T, N, K, KeyRSC, ANonce/SNonce/GNonce, MIC, GTK)

	설 명
S	EAPOL-Key Information Secure bit · 키교환이 완결되었음을 의미
M	EAPOL-Key Information Key MIC bit
A	EAPOL-Key Informaion Key Ack Bit
T	EAPOL-Key Information Key Install flag bit
N	EAPOL-Key Information Key index bit
K	EAPOL-Key Information Key Type Bit • Pairwise Key - P• Group Key - G
KeyRSC	EAPOL-Key KeyRSC field
ANonce SNonce GNonce	EAPOL-Key Key Nonce field
MIC	EAPOL-Key MIC field
GTK	EAPOL-Key Data field

표 3 EAPOL-Key message 매개변수

4. EAPOL Key Message Description in 4-Way Handshake

1) 4-Way Handshake protocol 개요

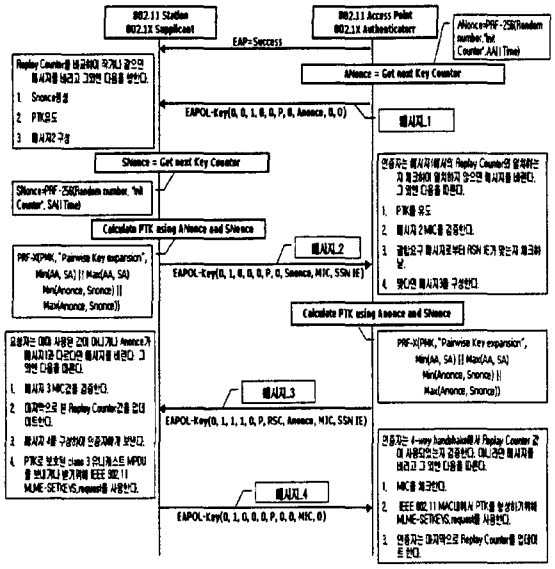

그림 3 4-Way Handshake

RSNA(Robust Security Network Association)은 4-Way Handshake라는 IEEE 802.1X protocol을 정의한다. 4-Way Handshake는 IEEE 802.11 link 위에서 다른 STA와의 직접 통신을 통하여 STA의 존재여부를 확인하고 공유된 session key가 신선한 것인지를 보증하며, 통신 중인 STA의 MAC 주소와 PMK를 결합시키고, IEEE 802.11 link의 안전성을 보장하기 위해 key의 사용을 동기화한다. IEEE 802.1X 인증과정은 4-Way Handshake로서 완료된다. 4-Way Handshake의 정보흐름은 다음과 같다.

가) 1 단계: 인증자 → 요청자에게 메시지_1전송
EAPOL-Key(0,0,1,0,0,P,0,ANonce,0,0)

나) 2 단계: 요청자 → 인증자에게 메시지_2 전송
EAPOL-Key(0,1,0,0,0,P,0,SNonce,MIC,RSN IE)

다) 3 단계: 인증자 → 요청자에게 메시지_3 전송
EAPOL-Key(0,1,1,1,0,P,IV,ANonce,MIC,RSN IE)

라) 4 단계: 요청자 → 인증자에게 메시지_4 전송
EAPOL-Key(0,1,0,0,0,P,0,0,MIC,0)

구체적으로 살펴보면

• EAPOL-Key()는 3장에서 소개된 형식을 사용하여 argument를 전달하는 EAPOL-Key 메시지를 나타낸다.

• ANonce는 인증자가 제공하는 nonce이다. 메시지 1과 3의 ANonce는 동일한 값을 갖는다.

• SNonce는 요청자가 제공하는 nonce이다. 메시지 2와 4의 SNonce는 동일한 값을 갖는다.

• P는 4-Way Handshake의 경우 1로 설정되며, 그룹 키의 경우 0으로 설정된다.

• MIC은 1에 정의된 MK를 사용하여 전체 EAPOL-Key 메시지에 대하여 계산된다. 최초 MIC 계산 시 내부 MIC 부분은 0으로 설정된다.

• RSN IE는 적절한 RSN IE를 기술한다.

4-Way Handshake 각 단계의 MIC 계산은 동일한 반면에 Ack bit는 각 방향마다 서로 다르다. Ack 비트는 인증자로부터의 메시지에는 1로 설정되고 요청자로부터의 메시지에는 0으로 설정된다. 요청자로부터의 4-Way Handshake 요청의 경우 Request bit는 1로 세팅된다. 요청자와 인증자는 reflection 공격을 막기 위해 Request 비트를 확인해야한다.

2) 4-Way Handshake 메시지

가) 메시지_1 : 요청자가 인증자로부터 메시지_1을 받으면 현재의 보안 결합에서 Replay Counter가 사용된 적이 있는지 여부를 판단한다. Replay Counter가 현재의 local 값보다 작거나 같다면 수신자는 그 메시지를 폐기한다. 그렇지 않을 경우 요청자는 새로운 nonce인 SNonce를 생성하여 PTK를 유도하고 메시지_2를 구성한다.

나) 메시지_2 : 요청자로부터 메시지_2를 수신한 인증자는 Reply Counter가 자신이 보낸 메시지_1의 Replay Counter와 일치하는지 체크한다. 만약 일치하지 않는다면 해당 메시지를 폐기한다. Replay Counter가 일치하는 경우 인증자는 PTK를 유도하고 메시지_2의 MIC을 검증하여 MIC 값이 일치하지 않으면 인증자는 해당 패킷을 폐기한다. MIC 값이 일치하는 경우 인증자는 RSN IE bit와 (재)결합 요구 메시지가 일치하는지를 체크하여 일치하지 않으면 인증자는 결합을 해지하기 위해 MLME- DEAUTHENTICATE.request를 사용하고 모두 일치하는 경우 인증자는 메시지_3을 구성하여 요청자에게 보낸다.

다) 메시지_3 : 요청자가 수신한 메시지_3에서 Replay Counter가 이미 사용된 값이 아니면 해당 메시지를 폐기한다. 또 ANonce가 메시지_1의 ANonce와 다른 경우 해당 메시지를 폐기한다. 이외의 경우 요청자는 RSN IE를 검증한다. STA가

수신하는 Beacon 또는 Probe Response내의 RSN IE와 일치하지 않으면 STA는 결합을 해지한다. 만일 이 메시지 내에 두 번째 RSN IE가 포함되어 있으면, 요청자는 두 번째 RSN IE에 규정된 unicast cipher를 선택하거나 결합을 해지한다. 만약 RSN IE가 정확하다면 요청자는 메시지_3에 대한 MIC을 검증하여 MIC 값이 틀리면 요청자는 메시지를 폐기하고, MIC 값이 일치하면 가장 최근에 사용된 Replay Counter의 값을 갱신한다. 요청자는 메시지_4를 구성하여 인증자에게 메시지_4를 송신한다. PTK로 보호된 class 3 유니캐스트 MPDU를 IEEE 802.11이 보내거나 받을 수 있도록 설정하기 위해 MLME-SETKEYS.request를 사용한다. 만약 메시지_4를 잃어버리거나 인증자가 메시지_3을 재시도한다면, STA는 MK와 temporal key로 보호된 응답을 다시 보낸다.

라) 메시지_4 : 요청자는 인증자에게 메시지_4를 보낸다. 이것은 PTK와 일치된 Temporal Key로 보호된다. 인증자가 메시지_4를 수신하면 Replay Counter 값이 현재의 4-Way Handshake에서 사용한 값인지를 검증한다. 만약 그렇지 않다면, 메시지를 폐기한다. 정당한 값이라면 인증자는 MIC을 체크하여 MIC 값이 틀리면 해당 패킷을 폐기하고 MIC이 정당하다면 2단계를 수행한다. IEEE 802.11 MAC에 PTK를 설정하기 위해 MLME- SETKEYS.request를 사용한다. 인증자는 자신의 Replay Counter를 갱신한다.

5. 결론

이것으로 IEEE 802.11i draft 4.0에서 제안된 키 체계와 키 분배 및 교환 메커니즘인 4-Way Handshake에 대해 살펴보았다. 이러한 4-Way Handshake 메커니즘에서 AP와 STA간의 상호인증 문제는 인증 서버가 AP에게 넘겨준 PMK로부터 STA와 AP에서 각각 계산된 PTK 값을 비교하여 상호인증을 수행 할 수 있다. 또한 동적인 키 문제에 있어서 이 메커니즘은 일정한 간격으로 PTK가 지속적으로 새롭게 생성됨으로써 Temporal Key가 공격자에게 노출이 되어도 안전한 통신을 지속할 수 있는 이점을 가지고 있다.

4-Way Handshake를 구현했을 시 다음과 같은 결과를 얻을 수 있다. 표 4에서 ANonce와 SNonce, PTK는 다음과 같이 계산된다. (그림 1과 표 1을 참조)

- ANonce = PRF-256(Random number, "Init Counter", AA|| time)
- SNonce = PRF-256(Random number, "Init Counter", SA|| time)
- PTK = PRF-X(PMK,"Pairwise key expansion", Min(AA,SA)||Max(AA,SA)||Min(ANonce,SNonce)||Max(ANonce,SNonce))

		16진수 Test Vector
PMK		0d c0 d6 eb 90 55 5e d6 41 97 56 b9 a1 5e c3 e3 20 9b 63 df 70 7d d5 08 d1 45 81 f8 98 27 21 af
AA		a0 a1 a1 a3 a4 a5
SA		b0 b1 b2 b3 b4 b5
SNonce		c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 d0 d1 d2 d3 d4 d5 d6 d7 d8 d9
ANonce		e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 f0 f1 f2 f3 f4 f5 f6 f7 f8 f9
PTK	MK	aa 7c fc 85 60 25 1e 4b c6 87 e0 cb 8d 29 83 63
	EK	ba 53 16 3d f3 2a 86 38 f4 79 ab e3 4b fd 2b c8
	TK1	8c b7 78 33 2e 94 ac a6 d3 0b 89 cb e8 2a 9c a9
	TK2	36 4a ff bb ce 87 5f 5d f2 dd 58 41 c0 ed 2a 41

표 4 4-Way Handshake Test Vector

참고문헌

[1] *Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification.* ANSI/IEEE Std 802.11, 1999 Edition

[2] *Wireless Medium Access Control (MAC) and Physical Layer(PHY) Specification: Medium Access Control(MAC) Security Enhancements.* Draft Amendment to ISO/IEC 8802-11/1999(I) ANSI/IEEE Std 802.11i/D4.0, 2003 Edition

[3] *Port-Based Network Access control.* IEEE Std 802.1x Standard for Local and Metropolitan Area Networks, June 14, 2001.