효율적인 키 갱신을 위한 무선랜 시스템의 암호 키 교환

강유성*, 오경희*, 양대헌*, 정병호*

*한국전자통신연구원, 정보보호연구본부

Cryptographic Key Exchange in Wireless LAN System for Efficient Key Refreshment

You Sung Kang*, Kyung-hee Oh*, DaeHun Nyang*, ByungHo Chung*

*Information Security Research Division, ETRI

요 약

초고속 무선인터넷 환경을 구축하기 위한 인프라의 강력한 대안이 되고 있는 무선랜 시스템은 사무실 단위의 소규모 네트워크 환경에서 벗어나 공중망 환경으로 진화하고 있다. 무선랜 시스템의 공중망 적용을 위한 주요 기술 중 하나는 무선랜 시스템의 보안성을 보장하는 것이다. 본 논문에서는 무선랜 사용자와 액세스포인트 사이에서 이루어지는 새로운 암호 키 교환 프레임을 제시하고, 그 결과로써 효율적인 무선구간 암호 키 갱신 및 보안성이 향상된 무선구간 데이터 프레임 암호화 효과를 보인다.

I. 서론

초고속 무선인터넷에 대한 요구가 급성장하면서 기존의 무선랜 (WLAN: Wireless Local Area Network) 시스템이 초고속 무선 공중망의 기반구조로써 그 대안이 되고 있다. 무선랜 시스템이 부각되는 이유는 이동통신 시스템이 가지는 낮은 전송속도를 극복할 수 있으며, 또한 무선랜 시스템의 보안 기술 개발이 활발하게 전개되면서 무선랜 사용자의 안전한 통신을 보장할 수 있으리라는 기대 때문이다.

IEEE 802.11 규격은 대표적인 무선랜 규격이다. IEEE 802.11 워킹 그룹은 2.4GHz 대역에서 DSSS 전송방식을 사용하는 IEEE 802.11b 규격, 5GHz 대역에서 OFDM 전송방식을 사용하는 IEEE 802.11a 규격, 그리고 전송속도 향상을 위한 고속의 무선데이터 전송방식을 연구하는 IEEE 802.11g와 같은 전송방식 연구 태스크 그룹과 더불어 무선랜 보안 기술 개발을 위한 IEEE 802.11i 태스크 그룹도 운영 중이다.

무선랜 시스템 보안을 위한 표준화 작업의 일환으로 IEEE 802.11i 태스크 그룹에서는 무선구간 데이터의 비밀성, 무결성, 메시지 인증을 위한 암호 키 교환 및 암호 알고리즘 적용을 정의하기 위한 논의를 진행하고 있으며, 사용자 인증, 접근제어, 신원확인 등의 절차는 IEEE 802.1 워킹 그룹에서 IEEE 802.1X 문서에서 정의하고 있다. 사용자 인증, 접근제어, 신원확인과 같은 기능은 무선랜 시스템 사업자와 인터넷 서비스 제공업체의 과금 정책을 실현할 수 있는 보안 요소로써 별도의 인증서버, 과금서버를 사용할 수 있다. 이렇듯 다방면의 보안 기능을 처리하여야 하는 IEEE 802.11 무선랜 시스템의 완전한 보안성 확보를 위하여 IEEE 802.1X 규격이 IEEE 802.1aa 문서의 내용을 추가로 가지게 되었으며, IEEE 802.11 워킹 그룹은 IETF의 인증서버 기술을 연동시키기 위하여 IETF 태스크 그룹과도 유기적인 협조를 취하고 있다.

본 논문에서는 IEEE 802.11 무선랜 시스템 중 무선랜 단말기와 액세스포인트(AP: Access Point) 사이의 무선구간 데이터의 비밀성, 무결성을 보장하는 무선구간 암호 키 교환을 위한 새로운 키 교환 메커니즘을 제안하고 그 효율성에 관하여 논한다. 본 논문의 구성은 다음과 같다. II장에서 일반적인 무선랜 보안 시스템을 보이고, 그 중 무선랜 단말기와 액세스포인트 사이의 무선구간 보안의 문제점을 설명한다. III장에서는 IEEE 802.11 무선랜 시스템을 보호하기 위한 무선랜 보안 표준화 동향을 살펴보고, 특히, IEEE 802.11i 태스크 그룹에서 발표한 문서에서 설명하고 있는 기존의 무선구간 암호 키 교환 메커니즘을 IV장에서 상세히 분석한다. V장에서는 본 논문에서

제안하는 새로운 키 교환 메커니즘을 상세히 설명하고 그 효율성을 논하며, 끝으로 VI장에서 결론을 맺는다.

II. 무선랜 보안 시스템

1. 무선랜 보안 시스템 구조

무선랜 사용자에게 무선인터넷 서비스를 제공하기 위해서는 무선랜 사용자의 데이터는 반드시 액세스포인트를 거쳐서 목적지 서버로 전달되어야 한다. 즉, 무선랜 시스템은 무선랜 단말기, 액세스포인트, 그리고 목적지 서버 등으로 구성될 수 있다. 그림 1은 이러한 무선랜 시스템 구성요소와 더불어 인증서버가 추가된 무선랜 보안 시스템 구성을 보여주고 있다.

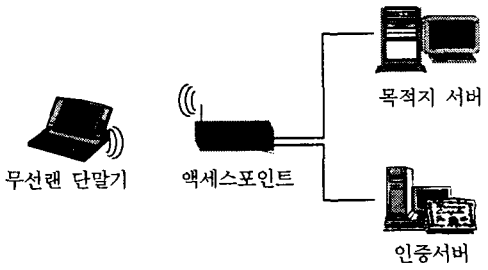

그림 1. 무선랜 보안 시스템

사용자 인증 측면에서 볼 때, 사용자는 우선적으로 인증서버로부터 인증을 획득한 후에 액세스포인트를 통하여 외부 인터넷망으로 접속이 가능하다. 데이터 보호 측면에서 볼 때, 무선랜 보안 시스템은 무선구간 보안과 유선구간 보안을 나누어 고려해야 한다. 유선구간은 무선랜 사업자가 관장할 수 있는 보안영역으로 존재할 수도 있으며, 현재의 유선인터넷 환경의 보안 기술이 적용될 수 있는 반면, 무선구간은 무선랜이 가지는 기본적인 브로드캐스팅 데이터 전송 특성으로 인한 무선 데이터 노출을 방어하기 위하여 암호 키 공유 및 암호 알고리즘 적용이 필수적이다.

2. 무선구간 보안의 문제점

무선랜 사용자와 액세스포인트 사이의 무선구간 보안성 파악을 위해 살펴보아야 할 것은 무선구간 데이터를 암호화하기 위한 암호 키 분배와 암호 알고리즘이다. IEEE 802.11 규격에서는 WEP(Wired Equivalent Privacy) 알고리즘을 사용하여 데이터 암호화를 수행하고, 그 암호 키는 미리 공유하여 고정적인 상태로 사용하도록 정의하고 있다[1]. 그러나 WEP 알고리즘은 IV(Initialization Vector)의 평문전송, 키 스트림의 단순성, 고정키 사용에 따른 RC4 키 갱신 부재 등으로 인해 키 길이에 상관없이 그 보안기능이 취약하다고 판명되었다[2]. 이러한 WEP 보안상의 취약점으로 인해 WEP 알고리즘을 사용하는 무선구간에서는 공격자가 암호문으로부터 평문을 유도할 수 있다[3].

따라서 IEEE 802.11 규격을 준수한 무선랜 시스템에서는 무선구간 보안을 위하여 상기의 취약점을 보완할 수 있도록 보안성이 강화된 새로운 암호 알고리즘의 정의와 동적인 키 분배 및 키 갱신에 대한 표준화 작업이 필요하다.

III. 무선랜 보안 표준화 기술

IEEE 802.11 규격의 무선랜 시스템에 대한 보안 기술 표준화와 관련된 대표적인 태스크 그룹은 IEEE 802.11 TGi이다. 또한 일반적인 포트기반 접근제어를 정의한 IEEE 802.1X 규격이 참조되며, 사용자 인증을 위한 메시지를 전달하는 확장 인증 프로토콜 (EAP: Extensible Authentication Protocol)과 인증서버 기술 역시 무선랜 보안 표준화를 위해 기술적 협의를 진행하고 있는 영역이다.

1. IEEE 802.11 TGi

IEEE 802.11i 규격은 IEEE 802.11 무선랜 시스템이 가지는 무선구간 보안의 취약점을 해결하고자 IEEE 802.1X 기반 접근제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 그리고 새로운 대칭키 암호 알고리즘의 적용 등을 그 내용으로 담고 있다[4]. 새로운 무선구간 암호 알고리즘으로는 TKIP(Temporal Key Integrity Protocol), WRAP(Wireless Robust Authenticated Protocol), 그리고 CCMP (Counter-Mode/CBC-MAC Protocol) 등이 있다.

2. IEEE 802.1X와 IEEE 802.1aa

IEEE 802.1X 규격은 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속 포트에 기반한 접근제어 기능을 정의하고 있다[5]. 무선랜 시스템에서도 이러한 포트기반 접근제어를 통해 무선랜 사용자 인증을 수행할 수 있으며, 무선구간 보안에 필요한 마스터 세션 키를 분배할 수 있다.

IEEE 802.1X의 포트기반 접근제어는 무선랜 시스템에서 사용자 인증을 처리하는 중요한 기능임에는 틀림없지만, IEEE 802.1X 규격은 무선구간의 보안을 위한 키 분배 문제를 명확하게 정의하지 않았기 때문에 IEEE 802.11i 문서에서 규정한 새로운 암호 알고리즘의 암호 키 설립을 지원하기 어렵다. 이를 보완하기 위하여 IEEE 802.1 워킹 그룹은 IEEE 802.1aa 문서를 발표했는데, 이 규격은 접속희망자(Supplicant)에 대한 인증과 더불어 무선구간 암호 키 분배를 위하여 IEEE 802.11i 규격의 키 서술자(Key descriptor)를 수용하고, 키 분배 상태 머신을 정의한 IEEE 802.1X의 수정 및 추가 문서이다[6].

3. EAP 프로토콜

무선랜 보안의 기본적 요구사항인 사용자 인증을 위한 프로토콜은 다양한 인증 프로토콜이 사용될 수 있다. 예를 들면, MD5-Challenge, TLS와 같은 일반적인 인증 프로토콜이 사용되어 무선랜 사용자와 인증서버 사이의 인증 기능을 수행한다. EAP 프로토콜은 무선랜 사용자와 인증서버 사이의 인증 데이터를 전달해 주는 확장 가능한 인증 프로토콜로 정의될 수 있다[7]. 즉, EAP-MD5, EAP-TLS, EAP-SRP, EAP-TTLS와 같은 형태로 무선랜 인증 프로토콜이 동작될 수 있으며, 이러한 EAP 메시지는 무선구간에서는 EAPOL (EAP Over LAN) 패킷에 실려서 교환되고, 유선구간에서는 RADIUS 프로토콜과 같은 별도의 인증정보 전송 프로토콜에 실려 교환된다. IEEE 802.1X의 포트기반 접근제어 구조에서는 액세스포인트가 제어 포트(Controlled port)와 비제어 포트(Uncontrolled port)의 두 개 포트를 유지하여 비제어 포트를 통해 이러한 EAP 인증 데이터를 인증서버로 전달하고, 인증 절차가 성공적으로 완료되면 제어 포트가 동작 가능 상태가 되어 무선랜 사용자가 해당 액세스포인트를 통해 무선인터넷 서비스를 받을 수 있게 된다.

4. 인증서버

무선랜 보안 시스템의 인증서버는 일반적으로 액세스포인트와 안전한 채널을 유지하며, 무선랜 사용자와 EAP 인증 메시지를 교환하여 인증 여부를 판단한다. RADIUS (Remote Authentication Dial In User Service) 서버가 대표적인 인증서버이며, 액세스포인트는 RADIUS 메시지를 생성하여 인증서버와 통신하는 RADIUS 클라이언트 역할을 수행한다[8].

IV. 기존의 키 교환 메커니즘

무선랜 보안 시스템을 무선구간과 유선구간으로 구분해서 고려할 때, 무선구간이 보다 더 심각하게 보안 취약점을 지니고 있다. 무선구간 보안을 위한 암호 키 교환은 특히 중요하게 논의되고 있는 기술적 고려사항이다. 본 장에서는 기존에 제안되고 논의된 무선구간 암호 키 교환 메커니즘을 설명한다.

1. 무선구간 암호 키 교환

IEEE 802.11i 규격에서는 무선구간 암호 키 교환을 위하여 4-단계 핸드쉐이크(4-way handshake)를 제안하고 있다. 그림 2는 4-단계 핸드쉐이크를 보여주고 있다.

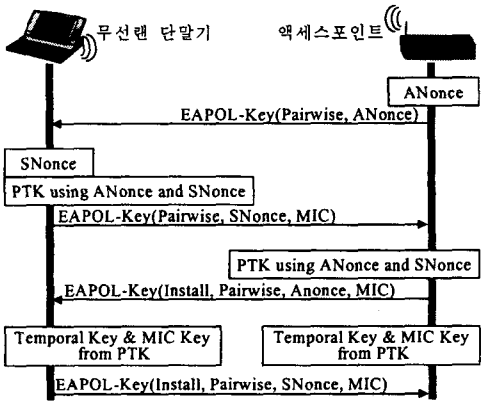

그림 2. 4-단계 핸드쉐이크 절차

무선랜 단말기와 액세스포인트는 EAP 인증 프로토콜을 통하여 마스터 세션 키를 공유하게 되면 위 그림과 같은 실제 무선구간에서 사용할 암호 키 교환 핸드쉐이크를 수행한다. 교환되는 주요 정보는 Nonce, Replay counter, IV, 그리고, 개별 키 (Pairwise key) 교환 또는 그룹 키 (Group key) 교환임을 나타내는 필드 등이 있다[4].

2. IEEE 802.11i 키 서술자

무선구간 암호 키 교환을 위한 4-단계 핸드쉐이크를 통해 교환되는 정보는 그림 3과 같은 IEEE 802.11i 키 서술자 구조로 전송되며, IEEE 802.11i 키 서술자는 EAPOL-Key 패킷에 실려서 교환된다.

개별 키 교환의 경우 실제 교환되는 무선구간 암호 키는 없으며, 상호 교환되는 Nonce 정보를 이용한 PRF (Pseudo Random Function) 동작으로부터 동일한 키를 공유한다. 그룹 키는 액세스포인트에서 생성되어 키 재료 필드에 담겨서 무선랜 사용자에게 전달되며, 그룹 키 전송 및 확인 절차는 4-단계 핸드쉐이크와는 별도로 진행된다.

Descriptor Type 1 byte	
Key Information	Key Length
Replay Counter 8 bytes	
Key Nonce 32 bytes	
Key IV 32 bytes	
Key MIC 16 bytes	
Key Material Length	Key Material

그림 3. IEEE 802.11i 키 서술자

3. 무선구간 암호 키 갱신

IEEE 802.11i 규격에서는 그룹 키의 키 업데이

트는 정의하고 있으나, 개별 사용을 위한 무선구간 암호 키 공유 이후에 개별 키의 갱신에 대한 언급은 없다. 비록 동적인 키 분배를 통해 매 세션마다 다른 키가 사용되지만, 하나의 세션에서 키 갱신이 이루어지지 않고 지속적으로 사용된다는 것은 보안상 취약점이 될 수 있다.

V. 제안된 키 교환 메커니즘

본 논문에서 제안하는 무선구간 암호 키 교환 메커니즘의 핵심은 IEEE 802.11i 키 서술자의 구조를 확장하여 이용한다는 것이다. 본 장에서는 효율적인 키 갱신이 가능한 확장된 무선구간 암호 키 교환 프레임을 제안하고, 그 효과를 분석한다.

1. 키 교환 핸드쉐이크

그림 4는 본 논문에서 제안하는 무선구간 암호 키 교환 프레임을 보여주고 있다.

Descriptor Type 1 byte		
Key Information	Key Length	
Replay Counter 8 bytes		
Key Nonce 32 bytes		
Key IV 32 bytes		
Key MIC 16 bytes		
Key Material Tag	Length	Key Value
Key Material Tag	Length	Key Value
...	...	...
Key Material Tag	Length	Key Value

그림 4. 제안된 키 교환 프레임

IEEE 802.11i 키 서술자의 필드를 그대로 준수한다. 그러나, IEEE 802.11i 키 서술자에서는 개별 키를 전송하지 않고 상호간의 PRF 동작으로써 개별 키를 생성해내는 반면, 본 논문에서 제안하는 구조에서는 그림 4의 음영 부분처럼 다수의 무선구간 암호 키들을 태그, 길이, 키 값 형태로 키 교환 프레임에 추가시킨다. 제안된 키 교환 프레임의 전송을 위해서 IEEE 802.11i 규격의 4-단계 핸드쉐이크 절차를 그대로 유지한다.

예를 들어, 첫 번째 태그는 WEP 알고리즘에 적용될 키, 두 번째 태그는 TKIP 알고리즘용 키, 세 번째 태그는 WRAP 알고리즘용 키, 네 번째 태그는 CCMP 알고리즘용 키, 그리고 다섯 번째 태그는 SEED 알고리즘용 키라고 정의한다. 만일 어느 임의의 순간에 데이터를 전송할 때, 세 번째 태그 값을 선행하고 태그 필드 뒤로 WRAP 암호화 데이터를 전송하게 되면 수신측에서는 태그 값을 인지하여 해당 암호 알고리즘과 암호 키를 이용하여 데이터를 복원해 낼 수 있다.

태그 필드가 선행하는 이런 형태의 데이터 전송은 선행되는 태그 필드에 대한 보호 대책이 요구될 수 있는데, 태그 필드를 보호하기 위한 암호 키로 무선랜 단말기와 액세스포인트가 공유하고 있는 마스터 세션 키를 사용하여 보호할 수 있다. 이 때 사용하는 암호 알고리즘은 미리 정해놓고 해당 알고리즘을 사용할 수 있으며, 또는 액세스 포인트가 하나의 태그 값을 선택해서 4-단계 핸드쉐이크 과정에서 무선랜 단말기에게 선택한 태그 값을 알려주면 해당 태그가 지시하는 알고리즘을 사용하는 방법이 있을 수 있다.

2. 무선구간 암호 키 갱신

IEEE 802.11i 규격에서 논의 중인 무선구간 암호 키 교환 방식이 사용하는 그림 3의 키 서술자 구조는 개별 키 교환 과정에서는 키 재료 필드가 존재하지 않으며, 또한 하나의 세션에서는 한번의 4-단계 키 교환 핸드쉐이크를 수행하여 단 하나의 무선구간 암호 키를 가지게 되므로 키 갱신이 어려운 구조적 약점을 지니고 있다. 그러나, 본 논문에서 제안하는 키 서술자 구조에서는 다수의 암호 키를 교환한 상태이기 때문에 만일 액세스 포인트와 무선랜 단말기 사이의 무선구간 암호 키 갱신이 요구된다 하더라도 이미 교환해 놓은 다수의 무선구간 암호 키 중에서 하나를 선택하여 태그 필드를 선행하고 해당 암호 알고리즘과 암호 키를 이용하는 형태로써 키 갱신을 수행할 수 있다. 이는 부가적인 키 서술자 교환 과정이 없이 효과적으로 무선구간 암호 키 갱신을 수행하는 방식으로 해석될 수 있다.

3. 다중 암호 키 적용

본 논문에서 제안된 키 서술자의 교환으로 생성된 다수의 무선구간 암호 키를 사용하여 전송 데이터 보안성을 향상시킬 수 있는 방법으로 각각의 전송 데이터를 각기 다른 암호 알고리즘을 적용하는 방법이 있을 수 있다. 즉, 송신측에서 전송 MSDU (MAC Service Data Unit) 각각에 대해 랜덤하게 선택된 태그 값에 따라 서로 다른 암호 알고리즘과 암호 키를 사용한다는 것이다. 이러한 다중 암호 키와 암호 알고리즘을 이용하는 무선구간 데이터 전송방식은 그 복잡도가 증가하는 단점이 발생할 수 있지만, 무선구간 공격자에게 암호 알고리즘도 노출되지 않게 되므로 무선구간의 보안 강도가 높아지는 효과가 있다.

VI. 결론

무선랜의 공중망 적용은 이미 현실로 다가왔다. 그러나, 현재의 무선랜 환경은 무선구간 보안에 큰 약점을 지니고 있다. IEEE 802.11 무선랜 규격에서 정의하고 있는 WEP 알고리즘의 보안 취약점이 밝혀짐에 따라 무선랜 사용자 인증과

더불어 보안성이 강화된 새로운 암호 알고리즘의 정의와 동적인 키 분배 및 키 갱신에 대한 표준화가 요구되고 있다.

본 논문에서 제시한 무선랜 사용자와 액세스포인트 사이의 새로운 암호 키 교환 프레임은 그 형태에 있어서 IEEE 802.11i 규격에서 논의되고 있는 키 서술자 구조를 준수하기 때문에 4-단계 핸드쉐이크에 적용될 수 있으며, 그 기능에 있어서는 개별 사용을 위한 무선구간 암호 키의 동적인 분배와 효율적인 키 갱신 효과를 기대할 수 있다. 또한 다수의 암호 키와 암호 알고리즘의 사용은 무선구간 보안 효과를 향상시킬 수 있을 것으로 예상된다. 향후에도 고속의 무선랜 환경을 보다 더 안전하고 믿을 수 있는 통신 채널로 유지하기 위하여 사용자 인증과 무선구간 보안 기술의 지속적인 연구가 필요할 것이다.

참고문헌

[1] IEEE, "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

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

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

[4] IEEE, "LAN/MAN Specific Requirements- Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Specification for Enhanced Security," IEEE Std 802.11i/D2.2, July 2002.

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

[6] IEEE, "Standard for Local and metropolitan area networks- Port-Based Network Access Control- Amendment 1: Technical and Editorial Corrections," IEEE P802.1aa/D3, July 2002.

[7] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 2284, March 1998.

[8] C. Rigney and et. al., "Remote Authentication Dial In User Service (RADIUS)," RFC 2138, April 1997.