무선랜 보안을 위한 새로운 키 관리 방식

이항석* · 이기영*

*인천대학교 정보통신공학과

New Key Control Metod for Wireless Lan Security

Hang-Seok Lee* · Ki-Young Lee**

*University of Incheon

E-mail : hangston2@naver.com

요 약

무선랜의 사용이 급격히 증가하고 있으나, 아직까지 대부분의 무선랜은 유선랜의 물리적 한계를 보완하기 위한 용도로 많이 사용되고 있다. 통신하는 두 사용자 간에 데이터를 암호화하여 보내면 이를 중간에서 가로채거나 변경이 불가능하게 되어 신뢰성이 보장된다. 하지만 사용자가 자의이든, 타의이든 암호화키를 유출하게 되면 신뢰성을 보장할 수 없게 된다. 그래서 암호화키를 안전하게 제공할 수 있도록 하는 키 관리 및 분배가 매우 중요하다. 본 논문은 보안에 취약한 무선랜의 사용에 있어서 기존 방식의 문제점을 살펴보며, 나아가 소규모 무선랜을 이용하는 사용자들을 위하여 키 관리와 분배기능을 하는 서버를 두고, 이를 통하여 보안상 문제점을 개선하기 위한 방안을 제공하려고 한다.

ABSTRACT

Wireless Lan is rapidly increased, but now most of wireless lan are being used to cover physical boundary of wired lan. If Users who communicate each other send cipher data, other users can not change or interrupt and the data is guaranteed for integrity. Otherwise, if user lose key for any reason, the data is not guaranteed for integrity. So it is important to control and manage to offer key. This Thesis examine problems of using existing wireless lan. Moreover, for users using small wireless lan, this offers installing server for controling and sharing and improves security problems.

키워드

Security, WLAN, Key, WEP

Ⅰ. 서 론

서비스가 지원되는 지역 내에서 위치에 상관없이 어디서든 접속할 수 있는 무선 통신 기술의 발전과 함께 컴퓨터 환경에서도 무선 네트워크를 이용하여 유선 환경과 통일한 서비스(Service)를 제공하고자 하는 것이 무선랜(WLAN : Wireless Local Area Network)이 등장하게 된 배경이다. 국내에서도 여러 통신서비스 사업자들이 공중 무선랜(Public WLAN) 서비스를 전개해 나가고 있어 무선랜에 대한 인지도와 무선랜의 사용이 증가하고 있다.

무선랜의 많은 장점인 이동성(Mobility), 유연성(Flexibility), 확장성(Extention), 효율성(Efficiency)에도 불구하고, 안전한 무선랜 보안 솔루션(Solution)은 상대적으로 취약하다. 무선랜은 무선매체(Wireless Medium)를 사용한다는 특성상 일정한 장비만 갖추어지면, 언제든 도청(Eavesdropping)이 가능하다. 그래서 무선랜 환경을 위한 기본적인 보안 서비스를 크게 세 가지 측면에서 지적할 수 있다. 첫 번째는 승인된 사용자에게만 네트워크 접속을 허용하는 인증

(Authentication)에 관한 보안이며, 두 번째는 스니퍼(sniffer)등을 이용해 무선랜을 통해서 전송되는 데이터에 대한 도청 행위를 방어할 수 있는 데이터 기밀성(Confidentiality)에 관한 보안이다. 마지막으로 데이터가 악의적인 스테이션에 의해 훼손되지 않았음을 보장하는 무결성(Integrity)에 관한 보안이다.

그래서 작은 규모의 무선랜을 사용하는 사용자들을 위하여 키 컨트롤러(Key Controller)를 이용하여 보안상의 문제점을 개선하기 위한 방안을 제공해 보도록 한다.

II. 802.11 보안 서비스의 취약점

802.11 보안 서비스는 대부분 WEP(Wired Equivalent Privacy) 프로토콜을 사용하여 제공한다. 그래서 WEP 프로토콜의 취약점이 802.11 보안 서비스 전체의 취약점이 된다. 이와 함께 WEP 키를 관리하는 메커니즘의 부재가 802.11 보안서비스의 가장 큰 취약점이다. 802.11 보안 서비스와 관련된 몇 가지 문제점은 다음과 같다.

2.1 RC4 알고리즘의 취약점

스트림 암호의 보안은 전적으로 스트림의 랜덤성에 의존하므로, 키 스트림의 재사용은 스트림 암호 기반의 시스템에서 큰 약점이다. 만약 동일한 RC4 키 스트림으로 암호화 되었다면, 두 암호화된 패킷의 XOR 연산은 두 평문 패킷의 XOR과 동일하다. 프레임 몸체의 구조와 함께 두 스트림의 차이를 분석함으로써 공격자는 평문 프레임 자체의 내용도 알 수 있다. 그래서 키 스트림의 재사용 방지를 위하여 WEP은 다른 RC4 키로 다른 패킷을 암호화 할 수 있도록 초기화 벡터(Initial Vector)를 사용한다. 그러나 초기화 벡터는 패킷 헤더의 부분이므로 암호화 되지 않으며, 도청자는 동일한 RC4 키로 암호화된 패킷에서 분리해 낼 수 있으므로 초기화 벡터도 알 수 있게 된다.

2.2 초기화 벡터 취약점

WEP에서 초기화 벡터는 메시지 중 암호화 되지 않고 전송되는 24비트 필드(field)이다. 이 24비트 스트림은 RC4 알고리즘에 의해 생성되는 키 스트림을 초기화하는데 사용하는 것으로 암호 목적으로 사용되기에는 상대적으로 필드가 작다. 이와 같이 초기화 벡터 공간은 매우 작으므로, 분주한 네트워크에서는 재사용될 가능성이 매우 높다.

2.3 WEP 취약점

표준화된 WEP 구현은 40비트의 공유 비밀키를 사용한다. 보안 전문가는 이러한 40비트 비밀키 길이의 적합성에 의문을 제기하였고, 그래서 업계에서는 104비트, 128비트의 WEP 키로 128 비트, 152비트의 RC4 키를 만들어 사용하고 있으나, 이런 긴 비트에 대한 표준은 만들어지지 않았다. 또한, 잘 설계된 암호화 시스템은 더 긴 길이의 키를 사용하면 추가된 키 길이만큼 키를 해독해 내는 시간이 늘어나는 추가적인 보안을 얻을 수 있으나, WEP 프로토콜은 잘 설계된 암호화 시스템이 아니므로, WEP 공격으로 잘 알려진 방법(AirSnort 등)을 사용하면, WEP 키의 길이에 상관없이 몇 초안에 비밀키를 찾아낼 수 있다.

2.4 CRC-32 Checksum 알고리즘의 취약점

WEP 프로토콜은 트래픽의 무결성을 위해 CRC-32 Checksum 알고리즘을 사용하고 있으나, 이 알고리즘은 암호학적으로 안전하지 않다. CRC-32 Checksum 알고리즘의 선형적인 성질을 이용하여, 공격자는 자신이 변조한 트래픽을 액세스 포인트(AP : Access Point)가 아무런 의심 없이 받아들이게 할 수 있다.

2.5 WEP 키를 사용한 인증 메커니즘 취약점

동일한 공유 비밀키인 WEP 키를 가지고 인증하는 것은 진정한 의미의 인증이라 볼 수 없다. 단방향 Challenge-Response 인증 메커니즘은 상호 인증을 제공하지 않아 스테이션은 액세스 포인트를 인증할 수 없어, 올바른 액세스 포인트와 통신을 하는지 확신할 수 없게 된다.

2.6 키 관리(Key Management) 메커니즘 부재

WEP는 키 분배에 치명적인 약점을 가지고 있다. WEP 키의 비밀 비트는 802.11 서비스 셋에 참여하는 모든 스테이션에 분배되어야만 한다. 그러나 802.11은 키 분배 메커니즘에 대한 스펙을 정하고 있지 않다. WEP 키를 분배하는 문제뿐만 아니라, 한번 설정한 키를 드물게 재설정하는 것 또한 공격자가 동일한 키 스트림으로 암호화된 많은 수의 프레임을 가지고 스트림을 조립할 수 있게 한다. 이러한 키 설정, 분배, 갱신에 관한 키 관리 메커니즘의 부재가 전체적으로 802.11 보안 서비스를 취약하게 만든다.

III. 제안하는 802.11 보안서비스 개선 방안

802.11에서 제공하는 보안 서비스 취약점이 발생하는 근본적인 이유는 키 설정, 분배, 갱신과 관련된 키 관리 메커니즘이 존재하지 않기 때문이다. 그래서 이를 개선하기 위한 방안으로 키 관리 구조를 제안한다. 제안된 방식을 사용하여 802.11 무선랜에서 안전한 통신을 하는 것이 본 논문의 궁극적인 목적이다.

여러 통신 서비스 사업자들이 공중 무선랜 서비스를 전개해 나가고 있지만, 대부분은 학교나 연구실 내의 작은 소규모 그룹단위로 무선랜을 구축해 사용하고 있다. 기존의 유선랜과 완전 별개의 서비스 형태로 무선랜을 사용하는 것이 아니라, 유선랜의 확장 또는 보완하는 차원으로 많

이 사용하고 있는 실정이다.

3.1 제안하는 키 관리 구조 모델

802.11에서의 보안 서비스를 강화하기 위한 방안으로 새로운 키 관리 구조 모델을 제안하기 위해 몇 가지 가정이 필요하다. 첫 번째로 현재 무선랜 사용 환경을 고려하여 공중 802.11 무선서비스가 아닌 여러 개의 기본 서비스 셋으로 이루어진 단일 확장 서비스 셋에 국한시킨 802.11 무선랜 환경이다. 그리고 이 확장 서비스 영역에는 하나의 키 컨트롤러만 존재한다. 두 번째로 스테이션은 무선 NIC를 장착한 랩톱이나 데스크톱을 말한다. 그래서 무선으로 데이터를 전송할 수 있다는 점만 제외하면 스테이션의 계산 능력은 기존 유선 환경에서 스테이션이 가지는 계산 능력과 동일하다. 세 번째로 무선 환경이라는 특성상 무선 NIC와 같이 무선에 접근할 수 있는 장비만 있으면 무선을 통해 전송되는 모든 트래픽을 암호화의 여부에 상관없이 도청할 수 있다. 그래서 항상 무선상의 트래픽이 도청 가능하다는 점을 고려하여 키 관리를 통한 데이터 기밀성을 보호하는 것에 가장 중점을 둔다. 네 번째로 액세스 포인트와 키 컨트롤러 사이의 유선 구간은 안전하다고 가정한다. 마지막으로 키 컨트롤러와 인증하기 이전의 스테이션과 액세스 포인트가 보내는 모든 트래픽은 키 컨트롤러를 거친다. 키 컨트롤러가 사전에 공유한 마스터키를 가지고 BSS(basic synchronized subset) 키와 암호화키를 생성하여 각 스테이션에 분배한 다음 인증 과정을 거치며, 이후 스테이션은 액세스 포인트를 통해 분산 서비스를 이용할 수 있다.

3.2 구성 요소와 역할

기존의 802.11 표준의 네 가지 구성 요소(분산 시스템, 액세스 포인트, 무선 매체, 스테이션)에 키 컨트롤러라는 개체만 하나 더 추가 되었다. 키 컨트롤러는 802.1x 표준이나 802.11i 스펙에 있는 Authentication Server와 비슷한 역할을 담당하지만, 가장 큰 차이점은 EAP 방법을 통해서 키를 생성하는 것이 아니라, 단일 확장 서비스 셋과 같은 작은 규모의 무선랜 서비스라는 점을 이용하여 컨트롤러가 직접 각 개체들(액세스 포인트와 스테이션)의 마스터키를 사전에 생성하여 인증과정을 거친 뒤, 오프라인(Off-Line)으로 분배한다는 점이다. 키 컨트롤러와 각 개체들 간 사전에 공유한 키는 긴 기간 동안 사용되는 마스터키의 역할을 담당하며, 이 키를 가지고 하나의 BSS에서 사용하는 BSS 키와 하나의 스테이션과 하나의 액세스 포인트만이 공유하는 각각의 공유키를 생성한다. 스테이션과 액세스 포인트의 인증에서 뿐만 아니라, 스테이션이 동일한 ESS내의 다른 BSS로 이동 시 사전 인증(Pre-Authentication)에도 사용된다. 그리고 BSS는 서비스를 받기 원하는 스테이션들의 그룹이므로 컨트롤러에 의해 생성된 BSS 키의 안전성은 기존 그룹의 키가 가지는 요구사항을 만족해야 한다.

BSS 키는 하나의 기본 서비스 셋이라는 그룹 내의 안전한 통신을 위해 필요하며, 그룹 키와 유사한 성질을 가진다. 그러므로 기존의 그룹 키가 가져야 하는 아래와 같은 네 가지 요구 사항을 만족해야 한다.

· BSS 키의 비밀성(Secrecy) : 공격자가 BSS 키를 도출해 내는 것이 계산상으로 불가능하여야 한다.

· 전방 비밀성(Forward Secrecy) : 공격자가 이전 세션의 BSS 키에 대한 정보를 알고 있더라도, 이후의 BSS 키를 계산할 수 없어야 한다.

· 후방 비밀성(Backward Secrecy) : 공격자가 이후에 알려진 BSS 키에 대한 정보를 가지고서 이전 세션의 BSS 키를 계산하지 못하여야 한다.

· 키 독립성(Key Independency) : BSS_1 키를 가지고 BSS_2 키를 계산하는 것은 불가능해야 한다.

위의 네 가지 성질들은 서로 연관성을 가지고 고려되어야 한다. BSS내의 스테이션 탈퇴 시 이후의 데이터에 대한 Forward Secrecy를 제공해야 하며, 새로운 스테이션이 BSS에 참여 시 이전의 데이터에 대한 Backward Secrecy를 제공해야 한다. 그리고 여러 개체들의 공모로 인해 BSS 키가 노출되는 것을 막기 위해 Key Independency도 제공되어야 한다.

3.3 마스터키 생성 및 분배

키 컨트롤러가 하나의 확장 서비스 셋에 있는 모든 개체들(액세스 포인트와 스테이션)에 대한 인증을 거친 뒤, MAC Address를 등록시키고, 표 1과 같이 키 컨트롤러가 선택한 난수와 각 개체들의 MAC Address의 해쉬값을 Seed로 사용하여 의사 난수 함수(PRF : Pseudo Random Function)를 통해 각 개체와 키 컨트롤러가 공유할 마스터키를 생성하여 그림 1과 같이 분배한다.

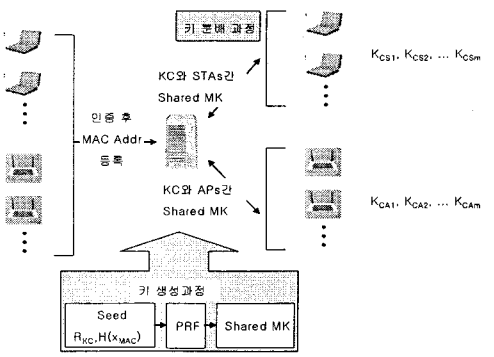

그림 1. 마스터 키 생성 및 분배 과정

· Seed(K_{C1}) = R_{KC},H($AP_{1,MAC}$) : K_{CA1}의 Seed
· Seed(K_{CS1}) = R_{KC},H($STA_{1,MAC}$) : K_{CS1}의 Seed
· K_{CA1} = PRF(Seed(K_{CA1})) : 키 K_{CA1}의 생성
· K_{CS1} = PRF(Seed(K_{CS1})) : 키 K_{CS1}의 생성

표 1 마스터 키 생성

3.4 BSS 키와 암호화 키 생성 및 분배

각각의 개체 (스테이션과 액세스 포인트)들은 키 컨트롤러로부터 자신들이 사용할 BSS 키와 암호화키를 전송받기 위해 사전에 키 컨트롤러와 · 공유한 마스터키를 사용하여, 파라미터(Parameter)들을 구성한 후 키 컨트롤러에게 전송한다. BSS키와 암호화키를 생성하고 분배하는 과정은 아래와 같이 전개된다.

① 스테이션(STA_1) ⇒ 액세스 포인트(AP_1)
M_{S2} = STA_1, N_{S1}
H_{S1} = HMAC(K_{CS}, M_{S1})

② 액세스 포인트(AP_1) ⇒ 키 컨트롤러(KC)
M_{A1} = M_S, H_S, AP_1, N_A
H_{A1} = HMAC(K_{CA}, M_{A1})

③ 컨트롤러에 의한 BSS 키의 생성
Seed(K_{BSS}) = R_{KC}, K_{CA}, H($AP_{1,MAC}$||$BSS_{1,ID}$)
K_{BSS1} = PRF(R_{KC}, K_{CA}, H($AP_{1,MAC}$))

④ 컨트롤러에 의한 STA1과 AP1 간의 암호화 키($K_{A1,S1}$)의 생성
Seed(K_{AS}) = R_{KC}, K_{CS1}, H($AP_{1,MAC}$||$STA_{1,MAC}$)

⑤ 키 컨트롤러(KC) ⇒ 액세스 포인트(AP_1)
$resM_{A1}$ = K_{CA1}(K_{BSS1}, K_{A1S1}, N_{A1})
$resM_{S1}$ = K_{CS1}(K_{BSS1}, K_{A1S1}, N_S, $AP_{1,MAC}$)
M_C = $resM_{A1}$, $resM_{S1}$

⑥ 액세스 포인트(AP1) ⇒ 스테이션(STA_1)
$resM_{S1}$,$K_{A1,S1}$($AP_{1,MAC}$)

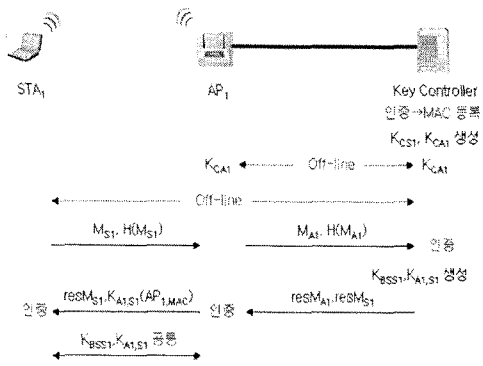

그림 2. 전체적인 키 생성 및 분배 과정

IV. 제안하는 키 관리 구조 모델의 안전성 분석

본 논문에서 제안하는 새로운 키 관리 구조 모델과 기존의 모델과의 가장 큰 차이점은 키 컨트롤러에 의해 생성된 마스터키가 사전 분배되고, 이 마스터키를 이용하여 BSS키와 각각의 스테이션 마다 무선 상에서 사용하는 자신들만의 고유한 암호화키를 유도해 낸다는 점과 키 컨트롤러에 의해 지속적으로 키가 갱신된다는 점이다. 또한, 무선 상으로 데이터를 전송할 시에는 BSS키를 선택적으로 사용하는 것이 아니라, 보안을 위해 강제적으로 사용하여야 한다는 점이다.

단일 ESS내의 모든 스테이션은 키 컨트롤러가 제공한 각각의 BSS키와 암호화키를 가지기 때문에 악의적인 스테이션 등은 트래픽을 복호화 할 수 없어 기밀성을 제공한다. 그리고 HMAC과 난수를 사용하여 무결성을 제공하며, 키 컨트롤러에게 마스터키를 제공받기 전에 오프라인으로 사용자 인증 과정을 거친다. 또한, BSS키, 마스터키, 키 컨트롤러에 의한 사용자 인증과정을 거쳐야 하므로 Man-in-the-Middle Attack, Session Hijacking으로부터 보호 받을 수 있다.

V. 결 론

IEEE 802.11 무선랜 서비스는 여러 장점으로 그 사용이 급격히 증가하고 있다. 그러나 이에 대한 보안은 상대적으로 취약하다. 그래서 보안서비스들을 정의하고 주로 WEP 프로토콜에 의해 제공되는데, WEP 프로토콜에 대한 많은 취약점이 발견되었다. 그리고 RSN을 통한 데이터 기밀성, 무결성을 위해 연구를 진행 중이지만 Man-in-the-Middle Attack, Session Hijacking에 노출될 가능성이 있다.

따라서 이를 해결하기 위한 방안으로 키 컨트롤러를 통한 새로운 키 관리 구조 모델을 이용하여 기밀성, 무결성, 인증과 함께 Man-in-the-Middle Attack, Session Hijacking에 대한 안정성도 함께 제공하고 있다. 그리고 마스터키를 사전에 분배하기 때문에 트래픽양도 줄어 소규모의 무선랜에 적합하다.

비록 새로운 디바이스의 추가시 항상 키 컨트롤러에 등록시켜야 한다는 단점이 있어 공중 무선랜에 비해 효율이 떨어지게 된다.

점차 확장되어가는 공중 무선랜에서도 이와 같은 키 관리 구조 모델을 공중 무선랜으로 확장 시, 이에 대한 고려사항 및 보안에 대하 연구가 필요하다.

참고문헌

[1] 김성철, 무선랜의 보안 취약점 및 안전성 강화 방안, 전남대 대학원, 2005
[2] 박지혜, 무선랜 통신보안 연구 : 무선랜 인증과 IEEE 802.11i의 메커니즘 분석, 국민대 대학원, 2003
[3] 홍성표, 강화된 사용자 인증 및 기밀성을 지원하는 무선랜 보안 시스템, 조선대 대학원, 2005