무선랜 보안 프로토콜 설계 및 분석에 관한 연구

심주걸*, 주미리**, 서인석**, 원동호***
*성균관대학교 전기전자및컴퓨터공학부
**국가보안기술연구소
***성균관대학교 정보통신공학부
e-mail:kmhrj@netian.com

A Study on the Design and Analysis of the Wireless LAN Security Protocol

Joo-Geol Sim*, Mi-Ri Joo**, In-Seog Seo**, Dong-Ho Won***
*Dept of Electrical and Computer Engineering, Sungkyunkwan University
**National Security Research Institute
***School of Inforl and Computer Engineering, Sungkyunkwan University

요 약

본 논문에서는 향후 네트워크 시장을 주도할 무선랜에서 암호화 기능과 인증 기능을 제공하기 위하여 제시된 보안 프로토콜인 WEP에 대하여 발견되는 취약점들을 지적하고 이에 대한 개선안을 제시하였다. 또한, 제시한 개선안을 토대로 초기 값 재사용을 방지할 수 있는 초기 값 생성 시스템과 블록 암호 CBC 모드를 이용하여 기밀성과 상호 인증 기능을 제공할 수 있는 새로운 무선랜 보안 모델을 제안하였다.

1. 서론

무선랜은 다양한 정보와 자원을 공유할 수 있게 하는 랜의 장점과 제약 없는 연결성 제공이라는 편리성을 동시에 제공하는 무선 통신 기술의 결정체로서, 신뢰성 있는 데이터 전송 뿐만 아니라 유연성과 설치의 용이성이란 장점으로 갖고 있다.

그러나, 무선이라는 특성은 편리함과 이동성이라는 장점을 제공하는 반면 모든 무선 단말에서 송·수신되는 데이터를 청취할 수 있으므로 무선랜을 이용하여 데이터를 전송하는 경우 정당한 송·수신자 이외의 제3자가 데이터를 알아볼 수 없도록 하는 기밀성과 정당한 사용자가 접속하였는지를 확인할 수 있는 인증 기능이 필요하게 되었다. 이를 해결하고자 무선랜 표준화 단체인 IEEE 802.11위원회에서는 암호화 기능과 인증 기능을 제공하는 WEP(Wired Equivalent Privacy)을 표준 권고안으로 발표하였다[1].

그러나 WEP은 암호문 생성 시 사용되는 초기 값 생성에 대한 구체적인 방법이 제시하고 있지 않으며, 초기 값의 크기 및 재사용 문제로 인하여 암호화를 하는 경우 안전성에 대한 문제가 제기되고 있다. 또한 메시지 인증을 위한 메커니즘이 안전하게 구현되지 못하여 메시지 변조·추가 공격 등에 취약할 뿐 아니라 정당한 키 소유만을 확인하는 일방향 인증 방식을 사용하고 있어 불법적인 인증 문제가 발생할 수 있다[2][3]. 현재, 세계 각국에서는 이러한 WEP의 취약점들에 대한 연구가 진행중이나 이를 대체할 새로운 모델은 아직 제안되지 못하고 있는 실정이다.

본 논문에서는 무선랜의 보안 프로토콜인 WEP에서 발견되는 취약점들을 지적하고 이에 대한 개선안을 제시하였다. 또한, 제시한 개선안을 토대로 초기 값 재사용을 방지할 수 있는 초기 값 생성 방법을 제안하였으며, 블록 암호를 기반으로 하는 안전한 무선랜 보안 모델을 제안하였다.

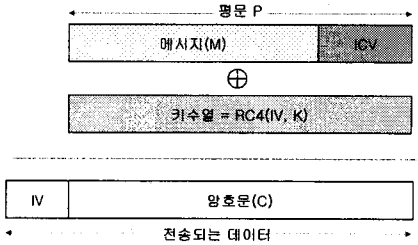
2. 무선랜 보안 프로토콜 WEP

2.1 WEP 암호화

무선랜을 이용하여 데이터를 실어 보내는 경우 기

밀성을 제공하기 위해서 제3자가 데이터 내용을 알 수 없도록 하는 암호 기능이 제공되어야 하며, 무선 네트워크에 정당한 사용자가 접속하는지를 검사하기 위한 인증 기능이 필요하다. WEP은 무선랜에서 암호 및 인증 기능을 제공하기 위한 프로토콜이다.

WEP에서는 스트림 암호 방식을 이용한다. 이때 사용되는 키수열은 의사 난수 생성기 RC4에 24비트 초기 값 IV와 40비트 비밀 키 K를 입력하여 생성된 2진 수열 $RC4(IV, K)$이다. 평문 P는 전송할 메시지 M과 메시지에 대한 CRC 검증값으로 구성된다. 암호문 C는 평문 P와 키수열 $RC4(IV, K)$를 XOR한 결과 값이다. 송신자로부터 수신자에게 전송되는 WEP 프레임은 $IV \parallel (P \oplus RC4(IV, K))$ 형태이다. 다음 (그림 1) WEP 프레임 구조를 나타낸다[1].



(그림 1) WEP 프레임 구조

2.2 WEP 복호화

WEP 프레임 수신자는 암호문 C와 초기 값 IV를 분리하고 초기 값 IV와 사전에 공유한 비밀키 K를 이용하여 키 수열을 생성한 후 메시지를 복호할 수 있다.

수신자는 사전에 공유한 40 비트의 비밀키 K와 수신한 WEP 프레임으로부터 분리한 24 비트의 초기 값 IV를 RC4에 입력하여 키수열 $RC4(IV, K)$를 생성한다. 키수열과 암호문을 Exclusive OR한 결과가 평문 P이다. 즉 암호문 C는 다음과 같이 복호된다.

$$C \oplus RC4(IV, K) = P \oplus RC4(IV, K) \oplus RC4(IV, K)$$
$$= P$$

수신자는 복호한 평문 P로부터 무결성 검증 값인 ICV를 분리하고 메시지 M을 CRC 알고리즘에 입력하여 ICV'를 생성한다. 그리고 생성한 ICV'와 ICV 값을 비교하여 수신한 메시지의 무결성을 확인한다. 만약, 값이 같으면 정당하게 전송된 메시지로 인정하고 틀리면 오류 메시지로 간주한다.

2.3 WEP의 취약점 및 개선안

무선랜의 보안 프로토콜인 WEP은 여러 가지 취약점이 지적되고 있다. 이는 WEP이 작은 크기의 초기 값을 사용하고 있어 재사용이 우려되며, 메시지 인증 기능이 없고 단지 오류 체크만이 가능한 CRC를 무결성 검증 값 ICV를 생성하는데 사용하고 있어 발생되는 문제점이다[3][4].

(1) 취약한 기밀성 제공

WEP에서 초기 값 IV와 비밀키 K가 재사용되는 경우 키 수열 소거 현상이 발생하여 암호문 단독 공격과 기지 평문 공격에 취약하다. 또한 초기 값 IV에 해당하는 모든 키 수열을 사전에 저장하면, 임의의 암호문 획득 시 해당 IV를 조회하여 실시간으로 평문을 해독할 수 있어 안전한 기밀성을 제공하기 어렵다.

개선안 1. 암호문 생성 시 매번 다른 초기 값을 사용한다. 이는 매번 다른 키수열을 생성할 수 있으므로 키수열 소거 현상이 발생하지 않는다.

개선안 2. 초기 값의 크기는 128 비트 이상이어야 한다. 128비트 이상의 크기를 가진다면 동일한 초기 값을 사용할 확률은 $1/2^{128}$이므로 안전하다.

(2) 취약한 메시지 인증 제공

WEP에서는 메시지 인증 방식으로 32비트 CRC checksum을 사용하고 있다. 그러나 CRC는 전송 도중 발생할 수 있는 random error에 대한 대책일 뿐이며, 악의 있는 공격자의 메시지 변조 공격에 대한 대비책이 되지 못한다.

개선안 3. 메시지 변조에 대한 방지책으로 메시지 인증을 위하여 MAC을 사용해야 한다. 단, MAC에 사용되는 키는 암호용 키와 동일하지 않다.

개선안 4. 초기 값을 재사용하지 않아야 하며, 메시지 인증은 반드시 비밀키를 이용하여 생성하는 MAC을 이용하여야 한다. 즉, 메시지 인증 값에는 비밀 정보가 들어가야 한다.

(3) 취약한 사용자 인증

공격자가 임의의 평문과 그에 해당하는 암호문 쌍을 알고 있다면, 불법적인 인증이 가능하다.

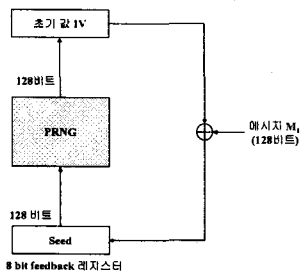
개선안 5. 시도 응답 방식을 사용해서 인증 프로토콜을 구성해야하며, 양방향 인증을 수행해야 한다.

3. 제안하는 무선랜 보안 프로토콜

3.1 제안하는 초기값 생성 시스템

WEP에서는 스트림 암호에 사용되는 키 수열을 만들기 위하여 40비트 비밀키 K와 24비트의 초기 값 IV를 사용하였다. 그러나, 초기 값 IV는 $1/2^{24}$의 충돌 확률을 가지고 있으므로 현재 시스템에서는 재사용의 가능성이 매우 높다.

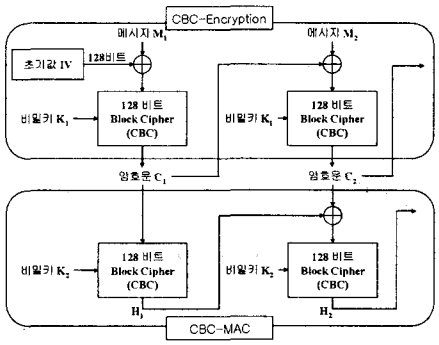
본 논문에서 제안하는 초기값 생성 시스템은 128비트 seed 값과 8 비트 피드백 레지스터를 이용하여 생성된 128비트 값을 의사 난수 생성기 PRNG에 입력하여 128비트 초기 값 IV를 생성한다. 이후 초기 값 IV의 재사용을 방지하기 위하여 암호화하고자 하는 메시지 M의 첫 번째 128비트 블록 M_1과 초기 값 IV를 Exclusive OR하여 그 결과 값을 8비트 피드백 레지스터에 입력 값으로 사용한다. 이때 사용되는 8비트 피드백 레지스터는 일련의 2진 수열을 발생시키기 위한 메커니즘으로, 레지스터 셀의 컨텐츠는 오른쪽으로 8자리 이동을 하고, 출력 시 8비트가 이와 같은 업데이트 과정에서 제거된다. (그림 2)은 의사 난수 생성기를 이용한 초기 값 IV 생성 방법을 나타내고 있다.



(그림 2) 제안하는 초기 값 생성 시스템

3.2 제안하는 무선랜 보안 모델

제안하는 무선랜 보안 모델은 블록 암호 알고리즘에 기반하고 있다. 128비트의 초기 값 IV가 128비트인 CBC(Cipher Block Chaining mode) 블록 암호 알고리즘을 사용하여 암호문을 생성하고, 메시지 인증을 위한 MAC은 CBC-MAC을 이용하여 생성한다. 제안하는 모델은 다음 (그림 3)와 같이 구성된다.



(그림 3) 제안하는 무선랜 보안 모델

3.3 암호문 및 MAC 생성

① 무선 단말은 128비트 초기 값 IV를 생성한 후 이를 128비트 블록 암호 ECB 모드를 이용하여 암호화한다. 이때 사용되는 비밀키 K_1은 암호문 생성 시에 사용되는 키와 동일하다.

$$E_{K_1}(IV)$$

② 평문 M은 128비트 (그림 3) CBC-Encryption을 이용하여 다음과 같이 메시지를 암호화한다. 이때 사용되는 비밀키 K_1이다.

$$C = E_{K_1}(M)$$

③ (그림 3)의 CBC-MAC을 이용하여 MAC값을 생성한다.

$$MAC = truncation(H_N)$$

④ 다음 값을 전송한다.

$$E_{K_1}(IV) \| C \| MAC$$

3.5 복호화

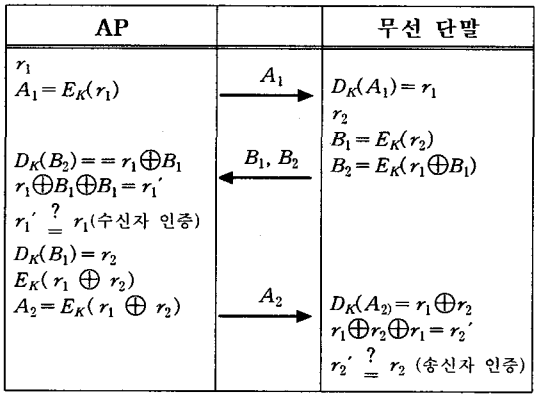
① AP(Access Point)는 $E_{K_1}(IV) \| C \| MAC$에서 MAC을 분리하여 암호문 C에 대한 무결성을 검증한다. MAC 값인 H_N에 오류가 발생하면 AP는 암호문을 복호하지 않고 오류 메시지를 무선 단말에게 전송한다.

② AP는 ECB 모드를 이용하여 초기 값 IV를 복호한다.

③ AP는 비밀키와 초기 값을 이용하여 암호문을 복호한다. 단, CBC 모드에서는 암호화된 순서대로 반드시 복호해야 한다.

3.6 상호 인증

AP와 무선 단말은 (그림 4)와 같이 각자가 선택한 임의의 난수를 암호화하여 서로에게 전달하는 시도 응답 방식을 이용하여 수신자 및 송신자 인증을 수행한다.



(그림 4) 상호 인증 프로토콜

4. 제안하는 무선랜 보안 프로토콜 분석

4.1 기밀성 제공

본 논문에서 제안하는 초기 값 생성 시스템으로 생성된 초기 값 IV는 재사용될 확률이 $1/2^{128}$이다. 또한 제안하는 블록 암호를 이용한 모델에서는 초기 값 IV를 ECB 모드를 이용하여 암호화하여 전송한다. 만일 공격자는 초기 값을 암호화한 비밀키를 획득하거나 전수 조사를 이용하여 초기 값 IV를 예측하는 경우 초기 값의 크기는 128비트이므로 전수 조사시 $1/2^{128}$ 확률로 계산될 수 있다. 이는 계산적으로 획득하기 불가능하다.

4.2 무결성 제공

제안하는 모델에서는 메시지 무결성과 출처 인증을 제공하기 위하여 CBC-MAC을 사용하였다. 이때 사용되는 초기 값 IV는 매번 바뀌며, 암호화할 때 사용되는 비밀키와 다른 비밀키를 이용하여 MAC 값을 생성한다. 따라서 메시지 추가 공격으로부터 안전하며, 특히 선택적 평문 공격에 안전하기 위하여 메시지를 암호화한 후 MAC을 생성하는 방법을 채택하였다.

4.3 상호 인증

제안한 방식에서는 송신자와 수신자가 블록 암호 방식을 이용하여 시도 응답 방식을 이용하여 인증을 수행한다. 또한 세 번의 통신으로 일방향 인증이 아니라 양방향 인증이 가능하다.

5. 결론

본 논문에서는 무선랜에서 보안 기능 제공하기 위하여 제안된 WEP이 가지고 있는 취약성을 분석하고 이에 대한 개선안을 제시하였다. 또한 제시한 개선안을 기반으로하는 초기 값 생성 시스템 및 블록 암호를 이용한 무선랜 보안 모델을 제안하였다.

제시한 초기 값 생성 시스템은 8비트 피드백 레지스터을 이용하며, 매번 다른 초기 값을 생성할 수 있어 초기 값 재사용을 방지할 수 있다.

또한 제안한 블록 암호를 이용한 무선랜 보안 모델은 안전한 기밀성과 무결성 및 상호 인증을 제공할 수 있다. 현재 기존의 WEP에 대한 취약성이 지적되고 다양한 대체 모델이 제시되고 있으나 아직까지 안전성이 증명된 시스템은 제안되지 않고 있다. 본 논문에서는 수십 년간 안전성이 증명된 CBC 모드를 사용한 블록 암호 기반의 보안 모델을 제시하였다.

참고문헌

[1] LAN MAN Standards Committee of the IEEE Computer Society, Wireless LAN medium access control(MAC) and physical layer(PHY) specification, IEEE Standard 802.11, 1999 Edition, 1999

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

[3] Walker. J., "Unsafe at any key size : an analysis of the WEP encapsulation", Tech, Rep. 03628E, IEEE 802.11 committee, March 2000. http ://grouper.ieee.org/groups/802/11/Documents/Document Holder/0-362.zip

[4] Borisov. N., I. Goldberg, and D. Wagner, "Interception Mobile Communications : The Insecurity of 802.11", In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, pp 180-188, 2001

[5] Walker. J., "Overview of 802.11 security", http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0p802-15_TG3%-Overview-of-802-11-Security.ppt, March 2001