홈 네트워크 무선랜 사용자를 위한 패스워드 기반의 인증 프로토콜

이주아O, 김재현
아주대학교 전자공학과

The Wireless LAN Authentication Protocol based on the Password for Home Network Users

Ju-A LeeO, Jae-Hyun Kim
School of Electrical and Computer Engineering, Ajou University
{gaia, jkim}@ajou.ac.kr,

요 약

본 논문에서는 홈 네트워크 무선랜 환경에서 접근제어를 설정하기 위하여 컴퓨터 및 보안 관련 지식이 없는 사용자라 하더라도 쉽게 무선랜 접근제어를 설정할 수 있는 기법을 고려하였다. 현재 사용되고 있는 복잡한 인증 설정 절차의 문제점을 해결하기 위하여 사용자의 개입을 최소화하기 위한 인증 시나리오를 제안하였다. 또한 주기적으로 랜덤하게 변경되는 패스워드를 사용함으로써 홈 네트워크 보안의 신뢰성을 높이고, 이를 지원하기 위하여 기존의 인증 프로토콜인 EAP 프로토콜을 바탕으로 하는 새로운 프로토콜을 제안하였다. 본 논문에서 제안하는 인증 프로토콜은 홈 네트워크 사용자에게 편리한 인증 방식을 제공하는 것뿐만 아니라, 기존의 프로토콜보다 신뢰성이 높아졌으며, EAP-MD5 프로토콜의 경우 brute force attack 과 replay attack 에 효과적으로 대응할 수 있다.

1. 서론

홈 네트워크는 다양한 통신기술들을 집약하여 사용자들에게 더욱 편리한 생활을 제공하기 위한 통합 기술 형 서비스이다. 홈 네트워크에서 제공되는 서비스는 에어컨, 냉장고 등의 가전 제품의 제어뿐만 아니라 상거래, 의료 서비스, 금융 서비스 등 개인의 신상 정보와 밀접하게 관련이 있다. 그러나 홈 네트워크에서 사용되는 유선랜에서는 물리적으로 연결된 단말들만이 랜 트래픽을 감지할 수 있는 것과는 달리 무선랜에서는 AP(Access Point)의 전송 반경 내에 있는 모든 단말기들이 다른 단말기 간의 송수신 데이터 내용을 감지할 수 있다. 이러한 문제점으로 인하여 이웃집간 무선통신 신호를 수신할 가능성이 높고, 집 외부에서 원하지 않는 사용자의 접근이 가능하므로 타인에 의하여 악용될 소지가 있다. 이에 따라 안전한 홈 네트워크 무선 통신을 위해서는 인가된 사용자만 인증하여 무선 자원을 이용할 수 있게 해주는 접근제어 기술이 필요하다.
IEEE 802.11 WG(Working Group)에서는 무선랜에서 사용되는 기본적인 인증 절차를 규정하고 있으나 이는 매우 기초적인 인증 절차로 악의적인 사용자의 접근을 차단하지 못하고 있다. IEEE 802.11i[1] TG(Task Group)는 무선랜 보안을 강화하기 위하여 IEEE 802.1X를 기반으로 하는 접근 제어 기법을 적용하고 있으며 동적인 키 교환 및 키 관리, 새로운 암호 알고리즘을 정의하고 있다. 이러한 새로운 보안 절차를 사용하기 위해서는 사용자가 무선랜 장치와 AP에 접속하여 필요한 정보들을 설정해야 하는 불편함이 있다. 그러나 홈 네트워크에서는 다양한 계층의 사용자들을 고려해야 하기 때문에 보안 및 컴퓨터에 대한 지식이 없는 사용자라도 홈 네트워크에서 쉽게 인증 방식을 설정할 수 있어야 한다. 본 논문에서는 사용자의 편의를 고려한 접근 제어 시나리오를 제안하며 홈 네트워크 특성에 맞는 인증 프로토콜을 제시한다.
2 장에서는 현재 사용되는 무선랜 인증 프로토콜에 대하여 살펴보며 3 장에서는 사용자의 편의를 고려한 접근 제어 시나리오와 인증 프로토콜을 제안하며 4 장에서는 제안한 접근 제어 시나리오의 성능에 대하여 평가하고 5 장에서 결론을 맺는다.

2. 무선랜 인증 프로토콜

2.1 IEEE 802.11i

IEEE 802.11i TG 에서는 접근 제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 무선 구간 데이터 보호를 위한 새로운 대칭키 암호 알고리즘의 적용 등을 정의하고 있다. IEEE 802.11i 는 IEEE 802.11 표준안에서 정의하고 있는 Open System Authentication 절차에 따라 승인이 완료되면, 사용자 인증을 위하여 IEEE 802.1X 프로토콜 절차를 따른다.

2.2 IEEE 802.1X

IEEE 802.1X 표준안은 논리적 포트 개념을 도입하여 링크 계층에서 IEEE 802 LAN을 인증하는 메커니즘을 제공한다[2]. 즉, 인증이 완료되기 이전에는 인증서버와 연결되어 있는 제어 포트(controlled port)를 통해서만 패킷이 전송될 수 있고, 인증이 완료된 이후에는 비제어 포트(uncontrolled port)를 통해서 외부 망과의 연결이 가능하다. IEEE 802.1X 표준안에서는 접근 제어를 위하여 요구자 (Supplicant), 인증자 (Authenticator) 및 인증서버 (Authentication Server)의 세 가지 개체가 정의된다. 요구자와 인증자 사이에서는 다양한 인증 방식을 수용할 수 있는 인증 프로토콜인 EAP(Extensible Authentication Protocol) 프로토콜을 통해서 인증을 수행하고, 인증자와 인증서버 간 통신 프로토콜은 별도로 규정하고 있지 않지만 RADIUS(Remote Access Dial-In User Service) 프로토콜에 대한 기본적인 참조 모델을 제시하고 있다.

2.3 EAP

IETF EAP WG에서 표준화를 진행하고 있는 EAP 프로토콜은 사용자 인증을 위하여 특정 인증 방식을 지정하지 않고, 여러 인증 방식을 지원하는 프로토콜이다[3]. 즉, EAP 자체로는 실제 사용되는 인증 프로토콜을 지정하지 않고, 단지 인증 프로토콜을 사용하기 위한 기본 절차만을 제공한다. 현재 표준화 중인 EAP 인증 방식은 EAP-MD5(Message Digest 5), EAP-TLS(Transport Layer Security), EAP-TTLS(Tunneled TLS) 등 여러 가지가 있으며 그 중 EAP-MD5 방식은 가장 초기의 인증 유형으로 패스워드를 기반으로하는 인증 방식이다. EAP-TLS[4]는 단말기와 인증서버가 인증서를 이용하여 상호 인증하는 방식이고, EAP-TTLS[5]는 EAP-TLS의 확장 형태로 서버는 인증서를 이용하여, 단말기는 패스워드를 이용하여 인증하는 방식이다.

3. 홈 네트워크에서의 인증 방식

3.1 접근 제어 시나리오

홈 네트워크 환경은 아이부터 노인까지의 다양한 연령대와 컴퓨터 및 보안 관련 지식이 없는 사용자를 고려해야 한다. 그러나 현재 홈 네트워크 내에서 무선랜 인증 방식을 이용하기 위해서는 사용자가 직접 네트워크 설정 윈도우 창에서 인증 정보를 설정해주어야 하는 불편함이 있다. 또한 인증 정보 설정은 관련 지식이 없는 일반 사용자가 사용하기에 어려운 전문용어로 구성되어있다. 이러한 점은 일반 사용자에게 신뢰성있는 인증 방식의 사용을 어렵게 하여 네트워크 보안에 심각한 문제를 야기할 수 있다. 특히 개인 정보 보안에 민감한 홈 네트워크에서는 사용자에게 보안에 관한 전문적인 지식을 요구하지 않고, 사용자의 개입을 최소화하면서도 신뢰성이 높은 인증 방식이 필요하다. 따라서 이와 같은 문제점을 해결하기 위하여 홈 네트워크 무선랜 사용자가 보안 및 컴퓨터에 관한 지식이 없더라도 쉽게 접근 제어 기법을 사용할 수 있는 시나리오가 필요하다.

홈 네트워크 내의 무선랜에서 사용자의 개입을 최소화하여 단말기를 인증하는 방법으로 인증서를 이용한 인증 방법이 거론되고 있으나[6], Bluetooth, Zigbee 등의 무선 통신 기술에서는 인증 프로토콜의 경량화가 요구되므로 인증서를 이용한 방식은 적합하지 않다. 본 논문에서는 무선랜에서의 인증 방식을 제안하고 있지만 홈 네트워크에서 사용될 다양한 무선통신 기술들과 관리의 용이성을 고려하여 패스워드를 이용하는 인증 시나리오와 이를 사용하기 위한 프로토콜을 제안한다.

사용자 입장에서 편리한 인증 방식을 제공하기 위하여 본 논문에서 제안하는 인증 시나리오는 사용자가 처음으로 사용하는 단말기에는 지정된 패스워드가 필요하다고 가정한다. 지정된 패스워드는 사용자가 인증서버에 직접 등록하거나, 단말기 판매점에서 단말기의 MAC 주소 정보를 홈 네트워크 서비스 사업자에게 전송하여 MAC 주소에 기반하는 패스워드를 홈 네트워크 인증서버에 등록시킬 수 있다. 이후에 인증서버는 패스워드를 랜덤하게 주기적으로 변경시켜, 인증된 단말기들에게 분배한다. 인증서버로부터 패스워드를 수신한 단말기들은 이후의 인증 과정에서 전송받은 패스워드를 이용한다. 이러한 과정들은 인증 과정에서 사용자의 개입을 최소화하거나 배제시켜 보안 지식이 충분하지 않은 사용자도 홈 네트워크의 안전을 보장받을 수 있다.

3.2 제안하는 인증 프로토콜

본 절에서는 인증서버에서 갱신한 패스워드를 어떻게 분배하고, 단말기는 어떠한 방법으로 새로운 패스워드를 이용하여 인증 받을 수 있는가를 정의한다.

제안하는 인증 프로토콜은 authentication number 라는 파라미터를 사용하여 이러한 문제점들을 해결한다. 패스워드가 변경 될 때 마다 랜덤한 숫자를 할당하고 이를 authentication number 라고 한다. 인증서버에서는 두 개의 테이블을 관리한다. 하나는 MAC 주소 관리 테이블로 인증된 단말기의 MAC 주소와 사용하고 있는 패스워드의 authentication number 를 기록해 놓는다. 다른 하나는 authentication number 관

표 1. 서버에서 운용되는 테이블

(a) authentication number 관리 테이블

authentication number	password
1	56789
3	12345

(b) MAC 주소 관리 테이블

MAC address	authentication number
EACB	1
ABCD	3

리 테이블이다. 패스워드가 변경 될 때마다 변경된 패스워드와 함께 랜덤한 authentication number 를 저장한다.

표 1 은 서버에서 운용하는 두 가지 관리 테이블의 예제를 보여주고 있다. 예를 들어 현재 홈 네트워크에서 사용되고 있는 패스워드는 표 1 (a)의 첫째 줄에 저장된 것과 같이 authentication number가 1 인 '56789'이다. 만일 MAC 주소가 EACB인 단말기가 처음으로 인증을 수행한다면 사용자가 지정한 패스워드를 통하여 인증을 수행한다. 처음으로 수행하는 인증이 아니라면 이전의 인증 과정에서 전송 받은 authentication number를 인증서버에게 전송한다. 예제에서는 MAC 주소가 EACB인 단말기가 전송한 authentication number는 1 이며 이 때, 인증서버는 전송 받은 authentication number인 1 과 MAC 주소 관리 테이블에 저장된 MAC 주소가 EACB인 단말기의 authentication number가 일치하는지 확인한다. 표 1 (b)에서 보는 바와 같이 EACB의 authentication number가 1 이므로, 인증서버는 authentication number 관리 테이블을 참조하여 authentication number인 1 에 대응되는 패스워드 '56789'로 인증 절차를 수행한다. 만일 현재 사용되고 있는 authentication number 가 1 이 아니라 표 1 (a)에서 보는 것과 같이 패스워드가 '12345'인 3 으로 변경되었다면 인증서버는 단말기에게 현재 authentication number와 패스워드를 전송한다. 그러므로 단말기는 이후의 인증 과정에서 변경된 패스워드로 인증을 받을 수 있다. 이와 같은 과정을 순서도로 나타내면 그림 1과 같다.

그림 2는 EAP-MD5 인증 수행 절차에 제안한 프로토콜을 적용한 그림이다. 그림 2에서 실선은 기존 프로토콜에서 사용하고 있는 메시지이며 점선은 제안하는 프로토콜에서 추가적으로 사용하는 메시지를 나타낸다.

자세한 인증 과정을 살펴보면 다음과 같다.

1. 802.11i 표준에 따라 Open System Authentication 이 완료되면 AP 는 802.1X 절차에 따라 단말기에게 ID 를 보낼 것을 요구한다. 단말기는 AP 에게 자신의 ID 와 함께 authentication number 를 전송한다.
2. 서버는 MAC 주소 관리 테이블에서 해당 단말기의 MAC 주소와 대응되는 authentication number 와 요청하는 authentication number 가 일치하는지 확인한다.

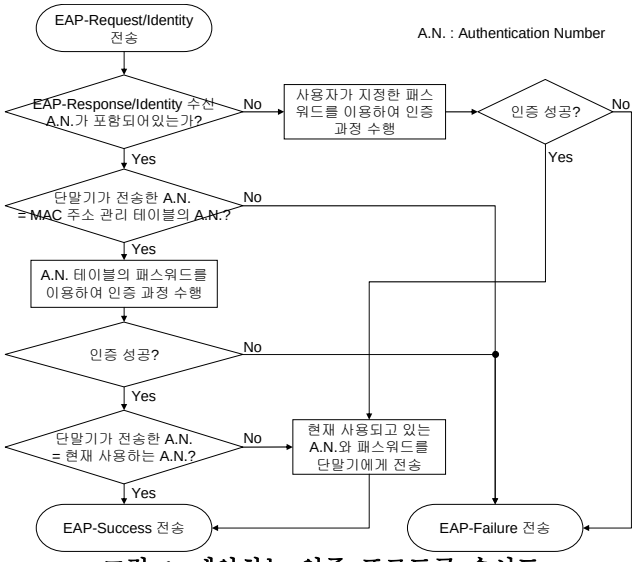


그림 1. 제안하는 인증 프로토콜 순서도

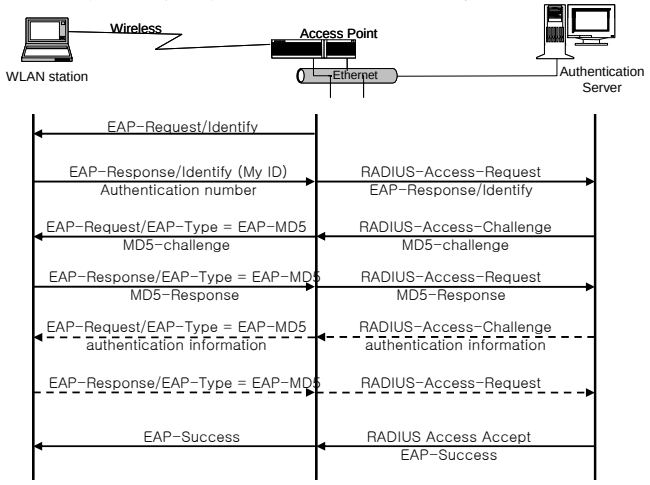


그림 2. 제안하는 EAP-MD5 인증 과정

3. 단말기가 요청하는 authentication number 가 적절하다고 판단되면 단말기에게 MD5-challenge 를 전송한다.
4. 단말기는 자신의 패스워드를 이용하여 MD5-challenge 를 암호화 한다.
5. 암호화된 MD5-challenge(MD5-Response)를 전송받은 인증서버는 authentication number 관리 테이블에 저장되어있는 해당 패스워드를 이용하여 이를 복호화 한다.
6. 서버는 복호화한 MD5-Response 와 전송했던 MD5-challenge 가 일치하는지 확인하여 단말기가 적합한 사용자인지를 결정한다.
7. 단말기가 적합한 사용자이고 현재 사용되고 있는 패스워드와 단말기에서 사용하고 있는 패스워드가 다르다면 서버는 authentication number 와 현재 사용되고 있는 패스워드를 단말기에게 전송한다. 이 때 중간에서 메시지 내용을 가로채지 못하게 단말기가 사용하고 있는 패스워드를 이용하여 인증 정보를 암호화하여 전송한다.
8. 단말기는 자신의 패스워드를 이용하여 전송받은 인증 정보를 복호화하고 인증 설정 정보를 변

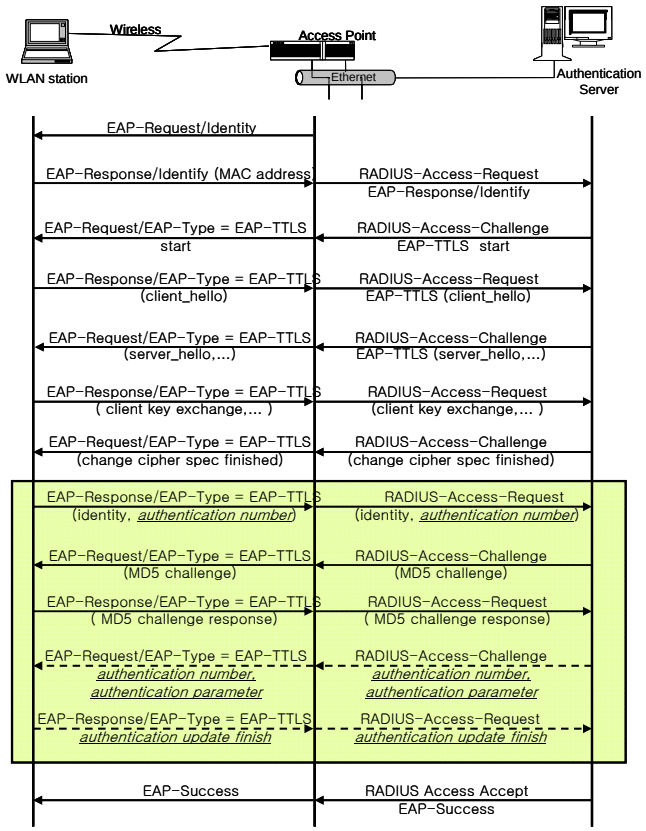


그림 3. 제안하는 인증 프로토콜

경하는 것과 동시에 인증서버로 EAP-Response 메시지를 전송한다.

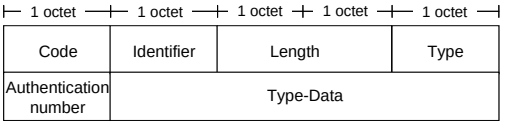
9. 인증서버는 EAP-Response 메시지를 수신하여 단말기가 변경된 인증 정보를 성공적으로 받았음을 알고 인증을 허락해주는 EAP-Success 메시지를 단말기에게 전송한다.

그림 3은 EAP-TTLS 인증 수행 절차에 제안한 프로토콜을 적용한 그림으로 실선은 기존의 메시지 교환을 나타내며, 점선은 제안한 프로토콜에서 추가된 메시지 교환을 나타낸다. 각 수행 절차에 대한 설명은 아래와 같다.

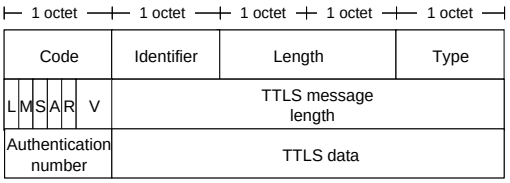
1. 802.11i 표준에 따라 Open System Authentication 이 완료되면 AP 는 802.1X 절차에 따라 단말기에게 ID 를 보낼 것을 요구한다. 단말기는 AP 에게 자신의 ID 대신에 MAC 주소를 전송한다.

2. 서버는 자신의 인증서 정보를 단말기에게 전송하여 단말기로부터 인증을 받고 이 때 생성된 키를 이용하여 TLS 연결(박스로 표시된 부분)을 만든다. TLS 연결 안에서 전송되는 메시지들은 키를 이용하여 암호화되기 때문에 중간에서 악의적인 사용자가 이를 가로채도 메시지의 내용을 알아낼 수 없다.

3. TLS 연결 안에서 인증 방식은 여러 가지가 사용될 수 있으나 본 절차에서는 MD5 방식을 사용하였다. EAP-TTLS 에서는 ID 정보를 TLS 연결 안에서 전송하여 개인 정보가 유출되지 않도록 보호해준다. 이 때, 제안하는 프로토콜에서는 ID 뿐만 아니라 authentication number 도 함께 전송한다.



(a) 제안하는 EAP-MD5 패킷 포맷



(b) 제안하는 EAP-TTLS 패킷 포맷

그림 4. 제안하는 패킷 포맷

4. 서버는 MAC 주소 관리 테이블에 해당 단말기의 authentication number 가 일치하는지 확인을 하고, 만약 일치한다면 authentication number 관리 테이블에 저장되어있는 패스워드를 이용하여 인증 절차를 수행한다.

5. 서버에서 단말기의 인증이 적합하다고 판단이 되고, 현재 사용되는 authentication number 가 단말기에서 전송한 authentication number 와 일치하지 않는다면, 단말기에게 현재 authentication number 와 해당 파라미터를 전송한다. 이 때 전송되는 정보는 TLS 연결에 의하여 안전하게 보호된다.

6. 단말기는 서버가 보낸 새로운 authentication number 와 파라미터를 전송 받으면 서버에게 응답 메시지를 보내고 서버는 EAP-Success 를 단말기에게 전송하여 단말기를 인증한다.

3.3 패킷 포맷

본 논문에서 제안하는 인증 프로토콜과 기존의 프로토콜과의 호환성을 위하여 패킷 포맷을 새롭게 설계할 필요가 있다. 그림 4 (a)는 제안하는 EAP-MD5 패킷 포맷을, (b)는 EAP-TTLS 패킷 포맷을 보여주고 있다. 패킷 포맷에서 Code 영역은 패킷을 Request, Response, Success, Failure 메시지로 구분하여 주며 Identifier 는 각 Request 에 대응되는 Response 를 인식하기 위한 영역이다. Type 영역은 Request 나 Response 메시지의 종류를 나타낸다. 예를 들어, Type 이 1 이라는 것은 identity 패킷을 나타내는 것이며, Type 이 13 이라는 것은 EAP-TLS 패킷임을 의미한다. EAP-TTLS 경우에는 많은 인증 정보가 EAP 패킷의 data 영역에 캡슐화된다. 캡슐화된 영역에서 L(Length included), M(More fragments), S(Start flag), R(Reserved), V(Version)는 flag 비트이다.

기존의 EAP-MD5 나 EAP-TTLS 프로토콜에 제안한 프로토콜을 적용할 경우, authentication number 는 사용자의 ID 와 같이 전송이 되지만 기존의 패킷 형식에서 인증서버는 ID 와 authentication number 를 구분할 수 없다. 그러므로 제안한 프로토콜의 파라미터는 호환성을 위하여 Type 영역과 R 비트를 변형시킨 패킷을 사용하여야 한다. authentication number 를 ID 와 같이 전송할 때는 새로운 Type 을 사용하여

데이터 영역에 실려서 전송이 되는 ID 와 authentication number 가 구분 가능하게 한다. 또한 EAP-TTLS 의 경우에는 기존 메시지의 R 비트를 A(Authentication number included) 비트로 사용하여 authentication number 전송 여부를 알릴 수 있어야 한다.

4. 성능 평가

4.1 신뢰성 분석(Security analysis)

제안하는 프로토콜은 사용자의 편의성뿐만 아니라 기존 프로토콜보다 보안 측면에서 뛰어난 성능을 보여준다. 특히 EAP-MD5 프로토콜은 다른 인증 방식보다 취약한 프로토콜로 여러 가능한 공격을 받을 수 있다. 그 중 하나인 brute force 공격은 공격자가 무선 구간의 스니핑을 통하여 사용자의 ID와 challenge, challenge-response를 수집하여 무작위로 패스워드를 대입하는 공격을 말한다. 현재 brute force 공격 툴을 이용하면 영문자의 대소문자와 숫자가 섞여있는 8 자리 이하의 패스워드를 알아내는데 1 주일이 소요된다. 따라서 brute force 공격에 대처하기 위해서는 영어의 대소문자와 숫자가 섞인 12 자리 이상의 패스워드를 최소한 1 개월 미만의 주기로 변경시켜야 한다[7]. 그러나 일반 사용자가 1 개월에 한번씩 12 자리 이상의 패스워드로 변경하는 것은 어려운 일이다. 제안하는 프로토콜은 자동적이고 주기적으로 변경되는 패스워드를 사용하고 있으며, 잦은 패스워드 변경에도 능동적으로 대처할 수 있도록 새로운 인증 파라미터를 추가하였기 때문에 더욱 안전하고 편리한 홈 네트워크 환경을 제공할 수 있다.

또 다른 공격 유형으로는 replay 공격이 있다. 공격자는 challenge 와 challenge-response 를 스니핑하여 목록을 만든다. 그리고 서버 또는 AP 가 목록에 있는 challenge 를 전송하면 스니핑한 challenge-response 를 전송하여 인증을 받는다. 그러나 제안하는 인증 프로토콜에서 단말기는 첫 번째 인증 이외에는 authentication number 를 서버에게 전송해야 하므로 공격자는 challenge response 를 전송하기 전에 일치하는 authentication number 를 전송해야 하는 어려움이 있다. 만일 공격자가 잘못된 authentication number 를 이용하여 공격을 시도한다면 서버는 공격 시도를 감지하여 공격에 대응할 수 있는 방안을 마련할 수 있다.

4.2 확장성(Scalability)

서버는 각 가정당 두 개의 테이블을 관리하므로 서비스 공급자 입장에서 운용하는데 부담이 될 수 있다. 따라서 제안하는 프로토콜이 추가적으로 요구하는 메모리 용량을 계산하여 볼 필요가 있다.

우선 MAC 주소 관리 테이블을 살펴보면 MAC 주소는 6byte 로 구성되며, authentication number 는 0 부터 255 까지라고 가정하였을 때 1byte 를 차지한다. 두 번째로 authentication number 관리 테이블에는 1byte 로 가정하는 authentication number 와 WEP2(Wired Equivalent Privacy 2) 키를 사용한다고 했을 때 가능한 패스워드는 16byte 로 구성될 수 있다. 이를 식으로 표현하면 다음과 같다.

$$total\ memory\ size = (6+1)\,bytes \cdot N_D + (16+1)\,bytes \cdot N_C \quad (1)$$

여기서, N_D 는 무선랜 단말기의 개수, N_C 는 authentication number 의 개수이다.

이 때 30 개의 무선랜 단말기와 100 개까지의 패스워드 정보를 저장한다고 가정한다면 관리테이블을 위한 총 메모리 크기는 1.91Mbyte 가 된다.

5.결론

본 논문에서는 홈 네트워크 무선랜에서 사용자를 고려한 편리하고 안전한 인증 방식을 제안하고 있다. 제안한 인증 방식은 사용자에게 전문적인 지식을 요구하지 않고, 자동적으로 패스워드 변경이 이루어지기 때문에 처음 인증 이후에는 사용자의 개입을 요구하지 않는다. 이는 다양한 연령 및 사용자 지식 수준을 고려해야 하는 홈 네트워크의 특성상 필수적으로 갖추어야 하는 점이다. 또한 본 논문에서 제안하는 패스워드의 주기적인 변경은 brute force 공격 및 replay 공격에 대응하여 무선랜의 보안을 좀 더 강화시킬 수 있다. 제안한 프로토콜에서는 이러한 인증 시나리오를 지원할 수 있도록 authentication number 의 사용과 기존의 프로토콜을 보완한 새로운 프로토콜을 제시하였다. 제안하는 프로토콜의 사용은 홈 네트워크 사용자에게 편리하고 안전한 환경을 제공할 것이다.

6. 참고문헌

[1] IEEE, LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification: Specification for Robust Security, IEEE Std 802.11i/D3.2, Apr. 2003.

[2] IEEE Standards for Local and Metropolitan Area Networks – Port-Based Network Access Control, IEEE Std 802.1X, Jun. 2001.

[3] B. Aboba et al., “Extensible Authentication Protocol,” IETF RFC 3748, Jun. 2004.

[4] B. Aboba, “PPP EAP TLS Authentication Protocol,” IETF RFC 2716, Aug. 1999.

[5] P. Funk, “EAP Tunneled TLS Authentication Protocol,” internet draft, Jul. 2004.

[6] D. Y. Yoo, Y. J. Won, H. Y. Youm, "Device certificate profile for the home network", ITU-T SG17 Meeting, Geneva Swiss, 5-14 October 2005.

[7] 김기태, “무선랜 개요 및 단순 공격 유형별 분석,” network times, 2003년 12월호.