단일 Bit 동기화를 이용한 무선 LAN에서의 효율적인 인증 프로토콜

조혜숙, 윤희용
성균관 대학교 정보통신 공학부
jojo@skku.edu, youn@ece.skku.ac.kr

An Efficient Authentication Protocol Using Single Bit Synchronization for Wireless LAN

Hea-Suk Jo and Hee Yong Youn
School of Information and Communications Engineering
SungKyunKwan University

요 약

오늘날 무선 LAN이 집안 또는 사무실, 산업현장, 공항 등과 같이 어디서나 무선으로 인터넷을 이용할 수 있게 설치되어 있다. 이런 무선 LAN 사용이 늘어나는 반면 보안상 결함을 해결할 보안 기능이 절실히 요구되는 실정이다. 본 논문에서는 무선 LAN환경에서 데이터를 안전하게 인증할 수 있는 효율적인 인증 Protocol을 제안한다. 여기서는 단일 Bit를 패킷에 추가하여 AP에서 확인 인증하는 방식을 채택하는데, 기존 방식과는 달리 AP에서 인증 스트림 동기화를 위한 작업을 수행한다. 컴퓨터 시뮬레이션이 최대 50%까지 기존 방식 보다 인증 스트림을 더 사용할 수 있게 하는 것을 보여주고 모바일 호스트의 전력 소모도 최소화한다.

1. 서론

무선 기술은 오늘날 사업 및 개인의 일상생활에서 점점 대중적으로 되어가고 있다. 예를 들면 PDA (Personal Digital Assistants)가 개인의 전화번호 명부, 주소 전자우편, 달력 및 인터넷에 접근하는 등 여러 가지 기능을 제공하고, GPS(Global Positioning System)는 세계의 어느 곳에 있는 장비도 그 위치를 알 수 있게 하는 기능이 있다. 그리고 휴대폰 등 Mobile 단말기와 무선 LAN을 이용한 인터넷 사용이 급증하면서 Mobile 뱅킹, Mobile 증권 거래나 인터넷 쇼핑몰 이용과 같은 무선 인터넷을 통한 전자상거래가 확산되고 있으며, 기업의 인트라넷/익스트라넷을 Mobile로 구축하는 사례 또한 빈번히 발생하고 있다.

이러한 무선 LAN 환경에서도 유선 인터넷과 마찬가지로 기밀성, 무결성, 부인 봉쇄를 달성할 수 있는 정보 보호 기술의 필요성이 절실한 상황이다. 무선 LAN을 이용한 망은 브로드캐스트 망이라는 특성상 도청(eavesdropping)이 쉽고, 무선 장비의 노출로 해킹이 용이하다. IEEE 802.11b 표준에서는 WEP(Wired Equivalent Privacy) 프로토콜과 같은 무선 LAN 보안 방법을 제안하였으나 키 스트림의 단순성으로 인한 실시간 공격, 도청으로 인한 평문 노출과 DoS 공격의 가능성, 동적인 WEP 키 분배 방법의 부재 등의 보안상 취약점이 드러났다[1]. WEP에서의 이러한 문제들을 해결하고 802.11b 보안을 위해 기업에서는 VPN 기술이 WEP에 추가하여 설치되어지고 있다.

그러나 IPsec/VPN과 WEP이 같이 사용됨으로써 보안으로서의 인증이 더욱더 강력해 지지만 인증 과정이 불필요하게 중복되는 과정을 거치게 된다. 이런 부분을 제거하기 위해서 본 논문에서는 IPsec/VPN을 사용하되 WEP을 대신하는 한 비트만을 추가함으로써 주고받는 데이터를 인증할 수 있는 효율

적인 인증 프로토콜을 제시한다. 여기서는 단일 Bit를 패킷에 추가하여 AP에서 확인 인증하는 방식을 채택하는데, 기존 방식과는 달리 AP에서 인증 스트림 동기화를 위한 작업을 수행한다. 컴퓨터 시뮬레이션이 최대 50%까지 기존 방식 보다 인증 스트림을 더 사용할 수 있게 하는 것을 보여주고 모바일 호스트의 전력 소모도 최소화한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 IEEE 802.11에서 사용되는 인증 방식에 대해서 알아보고 3장에서는 제안하는 인증 프로토콜에 대해 소개한다. 4장에서는 기존에 제안된 인증 프로토콜의 성능과 제시한 프로토콜의 성능을 평가 분석하고, 5장에서는 논문의 결론에 대하여 기술한다.

2. IEEE 802.11에서 사용되는 인증 방법 및 인증 프로토콜의 개요

2.1 IEEE 802.11에서의 인증방법[3]

2.1.1 Service Set Identifier(SSID)

SSID는 무선 랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로서, 무선 장치들이 BSS(Basic Service Set)에 접속할 때 마치 암호처럼 사용된다. SSID는 하나의 무선 랜을 다른 무선 랜으로부터 구분해 주므로, 특정 무선 랜에 접속하려는 모든 AP나 무선 장치들은 반드시 동일한 SSID를 사용해야만 한다. 특정 BSS의 고유한 SSID를 알지 못하는 그 어떠한 장치도 그 BSS에 접속할 수 없다. SSID는 패킷 상에 부가된 평범한 텍스트 데이터이므로, 충분히 스니프 당할 가능성이 있으며, 따라서 네트워크에 대해 어떠한 보증도 하지 않는다[4].

2.1.2 Media Access Control(MAC) Address Filtering

MAC이란 IEEE가 정의한 데이터 링크 계층의 두 가지 서브 레이어 중의 하위 레이어로서 OSI 7 계층중 데이터링크 계층의 주소로 네트워크카드의 48비트 하드웨어 주소를 말한다. MAC address는 LAN에 연결하는 모든 포트나 장치에 필요한 표준화된 데이터 링크 계층 주소이다. 전달되는 데이터에는 통신하는 하드웨어들 또는 AP와 STA 사이를 서로 인식하기 위해 사용하는 물리적인 애드레스가 부가되어 쓰인다. 이 물리 애어드레스를 바로 "MAC애드레스"라고도 한다.

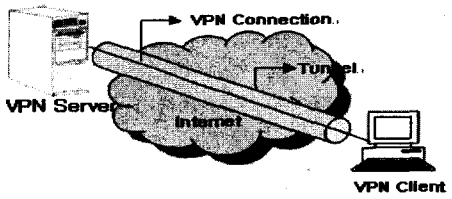
2.1.3 Wired Equivalent Privacy(WEP)

WEP은 유선 랜에서 제공하는 것과 유사한 수준의 보안 및 기밀 보호를 무선 랜에 제공하기 위하여 Wi-Fi 표준에 정의되어 있는 보안 프로토콜이다. WEP은 무선 랜을 통해 전송되는 데이터를 암호화함으로써 유선 네트워크의 물리적인 보안 대책에서 제공되는 것과 비슷한 방호를 제정하는 것을 추구한다. 데이터 암호화는 클라이언트와 AP 사이의 취약한 무선 링크를 보호하며, 일단 이 방법이 취해지면 기밀 보호를 확실히 하기 위해 암호 보호, 전구간 암호화, VPN 그리고 인증 등과 같은 다른 일반적인 랜 보안 절차들이 시행될 수 있다.

2.1.4 Virtual Private Network(VPN)

VPN은 공중 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하여 개별기업의 목적에 맞게 구성한 데이터 네트웍이다. VPN은 모든 회사들이 저마다 개별적으로 회선을 임차하는 것보다, 공중망을 공유함으로써 비용은 낮추면서도 전용회선과 거의 동등한 서비스를 제공하려는 아이디어에서 출발하였다.

가상 사설망은 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고, 수신측에서 복호화 한다(암호를 다시 푼다). 암호화는 데이터 뿐 아니라, 부가적인 차원의 보안으로서 송수신지의 네트웍 주소도 포함된다. (그림 1)은 VPN의 구조를 간단히 보여주고 있다.



(그림 1) VPN 구조

2.2 인증 프로토콜의 개요

앞에서 언급한 것과 같이 VPN은 현재 802.11 솔루션이 약한 지역을 보호하는데 사용한다. 최근 IEEE 802.11에서 IPSec AH/ESP, WEP 또는 AES+OCB와 같은 그룹은 데이터 패킷을 보호하는 강력한 인증 기술로 사용되고 있다.

기존에 제안된 인증 프로토콜[2] SOLA는 802.11에서 데이터를 액세스 할 때 동기를 맞춤으로해서 데이터를 인증하는 방법을 사용한다. SOLA(Statistical One-bit Lightweight Authentication)은 비용이 많이 드는 인증 기술대신 한 비트를 이용해서 인증

하는 방법이다. AP와 STA는 랜덤한 인증 스트림을 각각 가지고 있어서 이 랜덤한 값을 한 비트씩 MAC 레이어를 이용해 삽입하여 AP와 STA가 가지고 있는 스트림과 서로 비교하면서 인증하는 방식이다. 네트워크 환경에서는 데이터를 잃어버리기 쉽고 또 불법 사용자가 데이터를 중간에 빼낼 수 있는데 SOLA를 사용함으로써 이런 일들을 예방 할 수 있다

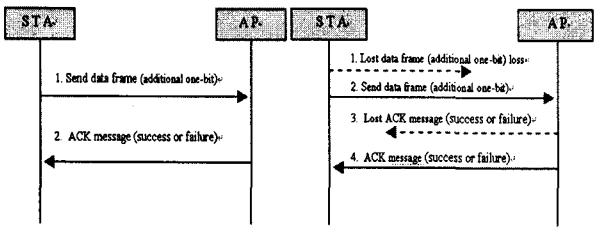
3. 제안하는 인증 프로토콜 연구

본 장에서는 WEP과 VPN 결합방식에서의 중복된 인증방식을 제거한 단일 비트 인증방법을 제안한다. 여기서는 네트워크 상에서 에러로 인해 데이터를 잃었을 때 동기를 맞추는 작업이 핵심 과제이다.

3.1 개 요

최근에 네트워크에서 보내지는 정보를 더욱 확실히 인증하기 위해 VPN과 WEP이 같이 사용되고 있다. 그러나 인증 과정에서 불필요하게 중복되는 부분이 생기게 되는 문제가 있다. 이를 제거하기 위해서 IPSec/VPN은 그대로 사용하고 WEP을 대체하는 인증 프로토콜을 제시한다. 여기서는 각 패킷에 한 비트만을 추가함으로써 주고받는 데이터를 인증하게 된다.

이 프로토콜의 주된 아이디어는 STA와 AP가 같은 인증 스트림을 갖고 있어서 데이터를 보낼 때, 인증을 위해 MAC-layer 헤더에 인증 스트림의 비트를 추가시켜 보내면 AP에서는 가지고 있는 인증 스트림과 보내온 비트가 같은지를 비교하며 데이터를 인증하는 방법이다. 그 예는 다음과 같다.



(그림 2) 왼쪽은 정상적인 인증과정, 오른쪽은 네트워크에서 에러 발생 시 인증과정

같은 초기값을 가지고 랜덤하게 만든 비트의 배열을 인증 스트림이라고 부르기로 하자. (그림 2)는 STA와 AP가 초기화된 인증 스트림을 이용해 데이터를 보내는 과정을 간략하게 나타낸다.

o 데이터 프레임을 성공적으로 보냈을 때

Step 1. STA에서 보낼 데이터 프레임에 한 비트를 추가하여 AP에게 보낸다.

Step 2. STA에서 받는 데이터에 있는 인증 비트와 AP의 인증 스트림에 있는 비트와 같은지 비교하여 같으면 STA에게 ACK-success를 보내고 다르면 ACK-failure를 보낸다.

o 데이터 프레임 또는 ACK를 잃었을 때

Step 1. 데이터 프레임을 보냈는데 불법 사용자가 가져가거나 네트워크 오류 때문에 소실되고 STA는 이 사실을 모르고 기다리게 된다.

Step 2. STA는 AP로부터 ACK 메시지가 오기를 일정시간 기다리다가 다시 데이터 프레임을 보낸다.

Step 3. AP가 데이터를 받고 인증 스트림과 비교한 후 ACK를 보냈는데 그 ACK를 다시 네트워크 상에서 잃었을 때 Step 2와 같이 STA가 데이터를 다시 보내게 된다.

Step 4. AP에서 데이터를 보내온 데이터 프레임을 받고 비트를 비교후 ACK 메시지를 보낸다.

3.2 동기 알고리즘

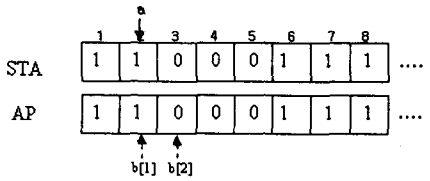
동기 알고리즘은 인증 스트림을 서로 맞추기 위해 사용된다. 기본적으로 STA와 AP는 인증스트림의 포인터를 움직이면서 각각의 비트를 체크하게 된다. 그런데 3.1절에서 보았듯이 STA나 AP에서 ACK를 잃었을 때 인증 스트림의 포인터가 맞지 않게 되어 문제가 생기게 된다. 일예로 AP는 ACK-success 메시지를 보내고 스트림의 포인터를 다음에 올 비트를 위해 한 비트 앞으로 움직이게 된다. 그런데 네트워크 상에서 ACK메시지가 손실된다면 일정 시간 후에 STA에서는 보냈던 비트를 한 번 더 AP에게 보내게 되고 따라서 동기가 맞지 않는 문제가 발생한다. 이런 경우 AP는 옮긴 포인터가 지시하는 값과 STA에서 다시 보낸 값을 비교하여 틀리면 동기를 맞추기 위해 비트의 포인터를 뒤로 움직이게 된다. 다음은 동기 알고리즘의 간략한 코드이다.

```
Algorithm for AP
//AP receives data packet with Bit[a]
if Bit[a] == Bit[b] then
   b++;
   AP->STA : Packet{ACK, success}
Else if Bit[a] ≠ Bit[b] then
 b--;
 AP->STA : Packet{ACK, failed}

Algorithm for STA
//STA receives ACK packet with success or
//failed bit from STA
if bit == success then
   a++;
End of Algorithm
```

(그림 3)은 ACK를 잃었을 때 동기를 맞추는 예이다. 그림에서와 같이 STA의 인증 스트림의 포인터

를 a라고 하고 AP의 포인터를 b[1], frame=2의 위치에 있다고 가정하자. STA에서 보낸 frame=2의 인증 비트 '1'과 AP의 비트가 같기 때문에 AP에서 ACK-success 메시지를 보내고 AP는 다음 비트(b[2])로 포인트를 위치시킨다. 그런데 ACK 메시지가 STA에게 보내어지는 도중에 손실됐다면 STA에서는 다시 a가 가르키는 비트를 보내게 되고 이를 받은 AP는 비트가 틀린 것을 알고 동기화시키기 위해 ACK-failed 메시지를 보내고 한 비트 뒤로 이동하게 되고 다시 a를 보냈을 때는 같은 비트로 동기가 맞게 된다.



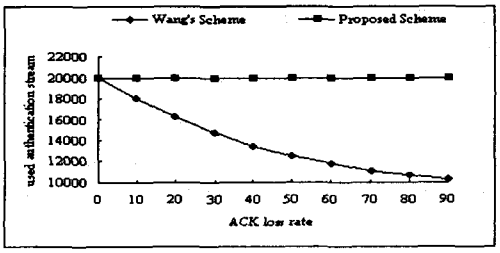
(그림 3) ACK를 잃었을 때 동기 맞추는 예

불법 사용자 인증 스트림을 추측해서 알아낼 확률에 대해서 보자. 인증 스트림은 0 아니면 1로 랜덤하게 배치되기 때문에 각각을 맞출 확률은 1/2 이다. 그래서 연속적으로 알아낼 확률은 점점 감소하게 되고 인증 스트림의 길이가 n이라면 이를 수식으로 나타내자면 2^{-n}으로 감소되게 된다.

4. 성능 평가 및 분석

본 절에서 제시하는 동기 알고리즘과 이와 비슷한 단일 Bit를 사용하는 동기 알고리즘(Wang's scheme[5])을 C 언어를 사용하여 시뮬레이션 한 결과를 성능평가 및 비교 분석 한다. Wang의 방식과 우리의 방식과의 가장 큰 차이점은 동기를 위한 포인터 위치 교정이 AP에서 일어난다는 것이다. 시뮬레이션은 20,000bit의 인증 스트림을 10번 수행한 결과 평균을 낸 값이다.

(그림 4)는 ACK를 네트워크 상에서 잃었을 때의 비율에 따라 인증 스트림의 사용 정도를 보여준다. 실제로는 ACK를 잃을 확률이 30%~90%까지 높게 나타나지는 않지만 비교 평가를 위해 넓은 범위의 에러율을 적용한 것이다. 그림에서 보이는바와 같이 기존에 제안된 Wang의 방식보다 우리의 방식에서 더 효과적으로 인증 스트림이 활용된다. WEP에서의 문제점 중 IV(Initialization Vector)를 모두 다 사용하였을 경우에 다시 할당하는데 걸리는 시간이 5시간 정도 걸리게 되는데 여기서 제안하는 프로토콜은 인증 스트림을 재 할당하는데 시간도 적게 걸릴뿐더러 기존에 있던 방식보다 더 효율적으로 사용하는 것을 볼 수 있다. 예를들어 20%의 ACK 에러율(네트워크상 손실율)로 인증 스트림의 사용을 보면 기존에 있던 방식보다 제안한 방식이 20%정도 더 효율적으로 스트림을 사용한다.



(그림 4) ACK를 잃었을 때의 인증 스트림 사용

5. 결론 및 향후 연구

본 논문에서는 IEEE 802.11 네트워크에서 접속할 때 효과적인 인증 프로토콜에 대해서 논하였다. 이 프로토콜은 두 스테이션 사이에 단지 한 비트만을 사용해 인증을 할 수 있고 기존의 방식보다 더 효율적인 것을 보였다. 효율적인 동기화 알고리즘을 이용하여 최대 50%까지 인증 스트림을 효율적으로 사용할 수 있다는 것을 시뮬레이션을 통해 검증하였다. 또한, 동기화를 AP측에서 맞춰 주기 때문에 모바일 스테이션 측에서의 전력소모를 최소화 할 수 있다는 장점도 있다.

많은 조직이나 기업체가 무선 환경을 이용하면서 강화된 보안 정책의 필요성을 느끼고 있다. 해커의 공격에 대한 보안, 부적절한 엑세스포인트의 활용 및 서로가 인증하는 사용자가 아닌 사용자에 대한 관리 점검, 무선 사용자의 전반적인 관리 등의 보안 개발 및 연구가 추가로 필요하다.

참고문헌

[1] M. M. Gast, "Seven Security Problems of 802.11 Wireless", O'Reilly Network, May, 2002

[2] H.Johnson, A.Nilsson, J.Fu, S.Felix Wu, A.Chen and H.Huang, "SOLA : A one-bit Identity Authentication Protocol for Access Control in IEEE802.11", In Proceedings of IEEE GLOBECOM, September 2002

[3] http://mail.terms.co.kr/

[4] Y.Yang, Z.Fu, Wu, S.F.,"Bands: an inter-domain inter-net security policy management system for IPSEC/VPN", Integrated Network Management, IFIP/IEEE Eighth International Symposium on,2003.

[5] Hao-li Wang, Aravind Velayutham, and Yong Guan, "A Lightweight Authentication Protocol for Access Control in IEEE 802.11", submitted to IEEE GlobeCom, Mar. 2003.