단일 Bit 동기화를 이용한 무선 LAN 환경에서의 효율적인 인증 프로토콜

조 혜 숙[†] · 윤 희 용[††]

요 약

오늘날 무선 LAN이 집안 또는 회의실, 교실 등과 같이 여러 장소에서 무선으로 인터넷을 이용할 수 있게 설치되어 있다. 이러한 새로운 환경은 보안에 관한 관심을 증대 시켰고, 최근에 강력한 인증 메커니즘 기반의 VPN과 WEP이 같이 사용되고 있다. 그러나 VPN과 WEP이 같이 사용됨으로써 보안성이 증가해 지지만 인증 과정에 불필요한 중복이 생기게 되고 그로 인한 전력소비 증가, 인증 속도 저하를 초래하게 된다. 본 논문에서는 인증을 하기 위한 메커니즘으로 간단한 인증방식, 모바일 스테이션의 적은 전력소비, 인증 스트림의 높은 이용율의 특징을 갖는 새로운 동기화 프로토콜을 제시한다. 이 프로토콜은 Access Point에서 각 프레임의 한 비트를 사용하여 인증하기 위한 동기화를 수행한다. 컴퓨터 시뮬레이션 결과, 새로운 동기화 알고리즘을 이용한 제안 방법이 기존의 비슷한 인증 프로토콜과 비교하여 인증 프레임 사용과 인증 속도 면에서 더 효율적임을 보이고 또한, AP측에서 동기화 과정을 수행하기 때문에 모바일 스테이션 측에서의 전력 소모를 최소화 할 수 있는 장점도 가짐을 보인다.

An Efficient Authentication Protocol Using Single Bit Synchronization for Wireless LAN Environment

Hea Suk Jo[†] · Hee Yong Youn[††]

ABSTRACT

Today, wireless LANs are widely deployed in various places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, etc. However, new concerns have been raised regarding security. Currently, both virtual private network(VPN) and WEP are used together as a strong authentication mechanism. While security is increased by using VPN and WEP together, unnecessary redundancy occurs causing power consumption increase and authentication speed decrease in the authentication process. In this paper a new synchronization protocol for authentication is proposed which allows simple authentication, minimal power consumption at the mobile station, and high utilization of authentication stream. This is achieved by using one bit per a frame authentication, while main authentication process including synchronization is handled by access points. Computer simulation reveals that the proposed scheme significantly improves the authentication efficiency in terms of the number of authenticated frames and authentication speed compared with an earlier protocol employing a similar authentication approach.

키워드 : VPN, WEP, 인증(Authentication), 동기화(Synchronization), AP(Access Point)

1. 서 론

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 전자 상거래가 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 망이므로 무선전파를 수신할 수 있는 영역 내에 있는 단말은 다른 사람의 송수신 데이터 내용을 청취할 수 있다. 따라서 무선랜에서는 데이터 프라이버시와 인증 서비스가 매우 중요하다. 이러한 특성상 도청(eavesdropping)이 쉽고, 무선 장비의 노출로 해킹이 쉽게 이루어진다. IEEE 802.11b 표준에서는 WEP(Wired Equivalent Privacy)

※ 이 논문은 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업과 2003년도 두뇌한국21사업의 지원에 의하여 연구되었음.
† 준 회 원 : 성균관대학교 대학원 컴퓨터공학과
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2004년 5월 13일, 심사완료 : 2004년 9월 15일

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 IPSec/VPN 기술이 WEP과 추가되어 설치되고 있다[8]. 그 이유는 IPSec은 네트워크 계층에서 제공되어지고 데이터링크 계층(WEP 사용)과는 독립되어있기 때문이다.

IPSec/VPN과 WEP이 같이 사용됨으로써 보안성이 증가해 지지만 인증 과정이 불필요하게 중복되는 과정을 거치게 된다. 이런 부분을 제거하기 위해서 본 논문에서는 IPSec/VPN을 사용하되 WEP을 대신하여 한 비트만을 추가함으로써 주고받는 데이터를 인증할 수 있는 효율적인 인증 프로토콜을 제시한다. 최근에 발표된 SOLA(Statistical One-bit Lightweight Authentication)의 단일 비트를 이용한 인증방법과 유사한 방식을 사용하는데 본 논문에서 제안된 방법이 더 효율적이고 능률적인 방식임을 보여준다. 단일 비트를 패킷에 추가하되 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 증명하고 또한 모바일 호스트의 전력 소모도 최소화한다. 새로이 제안된 동기화 프로토콜의 주된 특징을 보면 다음과 같다.

- 강력한 인증 : 강력한 인증 방식으로 공격(Denial-of-Service attack, overwrite attack, Man-in-Middle attack)을 검출할 수 있다.
- 간단한 인증 : 무선 네트워크와 같은 환경에서 단지 단일 비트를 사용함으로써 사용자 인증을 할 수 있다.
- 모바일 스테이션의 전력 최소화 : 제안된 인증 프로토콜을 이용하여 AP에서 확인 인증하는 방식을 채택하여 한정된 전력을 가지고 있는 모바일 스테이션의 전력 소모를 최소화 할 수 있다.

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.

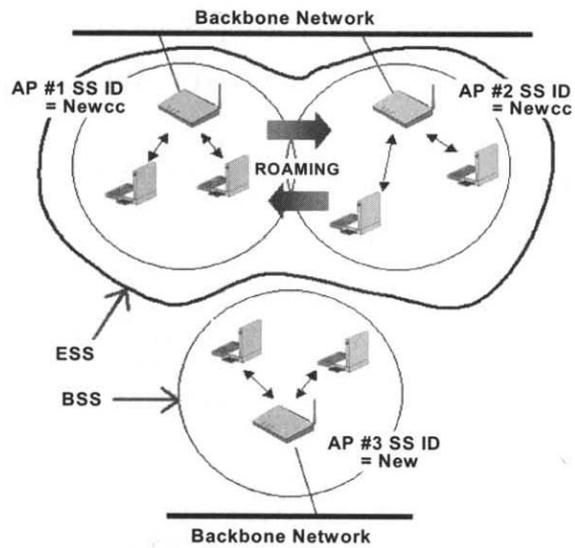
2. 관련 연구

2.1 IEEE 802.11에서의 인증방법[3]

IEEE 802.11b 표준은 서비스 세트 식별자(SSID : Service SetIdentifier)와 WEP(Wired Equivalent Privacy) 등 무선 LAN에서 액세스 제어와 프라이버시를 제공하는 두 가지 메커니즘을 정의한다. 암호화를 통해 프라이버시를 보호하는 또 다른 메커니즘으로 무선 LAN에서 투명하게 실행되는 가상 사설 네트워크(VPN)에 대해서도 살펴본다.

2.1.1 Service Set Identifier(SSID)

통상적으로 사용되는 무선랜 기능 중에 SSID는 초보적인 수준의 액세스 제어를 제공한다. SSID는 일반적으로 보안이 잘 되어 있지 않기 때문에 액세스를 승인/부인하는 방법으로서 SSID를 사용하는 것은 위험하다. 무선 클라이언트를 유선 LAN에 연결하는 장비인 액세스 포인트(Access Point, AP)는 일반적으로 SSID를 전파 탐지기에서 브로드캐스팅 할 수 있도록 설정된다. 예를 들어 무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32바이트 길이의 고유 식별자는 무선 장치들이 BSS(Basic Service Set)에 접속할 때 마치 암호처럼 사용된다. SSID는 하나의 무선랜을 다른 무선랜으로부터 구분해 주므로, 특정 무선랜에 접속하려는 모든 AP나 무선 장치들은 반드시 동일한 SSID를 사용해야만 한다. 특정 BSS의 고유한 SSID를 알지 못하면 그 어떠한 장치도 그 BSS에 접속할 수 없다. SSID는 패킷 상에 부가된 평범한 텍스트 데이터이므로, 충분히 스니핑 당할 가능성이 있으며, 따라서 네트워크에 대해 보안을 제공하지 못한다[4, 6, 9].



(그림 1) SSID 구조

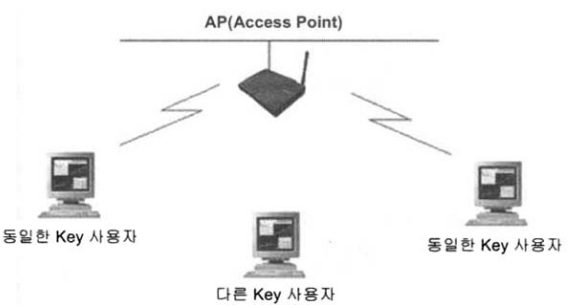
2.1.2 Media Access Control(MAC) Address Filtering

MAC이란 IEEE가 정의한 데이터 링크 계층의 두 가지 서브 레이어 중의 하위 레이어로서 OSI 7계층 중 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 애드레스를 바로 "MAC애드레스"라고도 한다. 보안 향상을 위해, 각 AP는 AP로의 액세스가 허용된 클라이언트 컴퓨터와 관련된 MAC 애드레스 목록을 갖고 있다. 만일 클라이언트의 MAC 애드레스가 이 목록에 존재하지 않는다면, AP는 액세스를 거부하게 된다. 이러한 방법을 통해 보안 기능을 향상시킬 수 있지만 이는 비교적 소

형 네트워크에 적합한 방법이다. 유입되는 MAC 애드레스에 대한 처리와 AP 디바이스의 최신 목록 유지가 확장성에 제약을 주게 된다[7, 11].

2.1.3 Wired Equivalent Privacy(WEP)[6]

IEEE 802.11b 표준은 유선 동등 프라이버시(WEP)라 불리는 선택적 암호화 방식을 정의하는데, WEP는 무선 LAN 데이터 스트림을 보호하는 메커니즘을 제공한다. WEP는 동일한 키와 알고리즘을 사용하여 데이터를 암호화하고 해독하는 대칭적 알고리즘을 사용한다. 클라이언트는 인증 받기 전에는 무선 LAN에 참여할 수 없다. IEEE 802.11b 표준은 개방형 키와 공유키 등 두 가지 방식의 인증 방식을 정의한다. 인증 방식은 각 클라이언트에 설정되어야 하며, 그 설정은 클라이언트가 연결하려는 액세스 지점의 설정과 일치해야 한다. 개방형 인증은 기본 사항으로서, 전체 인증 프로세스는 클리어 텍스트에서 이루어지며, 하나의 클라이언트는 정확한 WEP 키를 제공하지 않는 경우에도 액세스 지점과 연결할 수 있다. 공유 키 인증의 경우 액세스 지점은 클라이언트가 정확한 WEP 키를 사용하여 암호화하고 액세스 지점에 다시 반환해야하는 챌린지 텍스트 패킷(challenge text packet)을 클라이언트에 보낸다. 클라이언트가 잘못된 키를 갖고 있거나 키를 갖고 있지 않으면 인증에 실패하고 AP에 연결할 수 없다.



(그림 2) WEP 방식

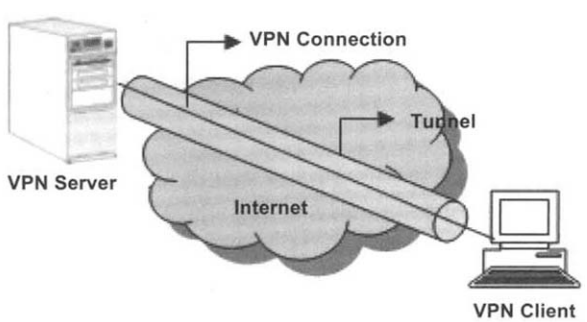
WEP 보안은 RSA 데이터 시스템의 RC4라 불리는 암호화 알고리즘을 토대로 하고 있는데 최근 RC4 암호에는 취약점이 있는 것으로 나타났다. 대표적인 공격 사례가 네트워크 키 획득을 위해 RC4의 키 스케줄링 알고리즘의 약점을 이용한 것이다. 무선 랩톱의 인터넷에서 얼마든지 쉽게 구할 수 있는 소프트웨어를 가진 사람이면 누구나 15분 이내에 무선랜에 대한 액세스가 가능하다는 것이 입증되었다. WEP 보호 자체만으로는 불충분하다는 것이 증명된 것이다[7].

2.1.4 802.1x[14]

IEEE 802.1x 표준은 802 LAN에 사용되는 일반적인 인증 구조를 제공하며 여러 가지 종류의 인증 프로토콜에 대해 LAN 전송을 가능하게 하는 확장 인증 프로토콜(EAP)을 지정한다. WAN 클라이언트는 액세스 지점으로 인증 요청을 시작하고, 액세스 지점은 확장 인증 프로토콜(EAP) 규격 RADIUS 서버로 클라이언트를 인증한다. 이 RADIUS 서버는 사용자(암호를 통해) 또는 컴퓨터(MAC 주소를 통해)를 인증할 수 있다. 802.1x 인증은 802.11 인증 프로세스와는 별개의 인증이다. 802.1x 표준은 인증 프레임워크를 제공한다. 802.1x 인증 유형은 여러 가지가 있으며 각각 다른 인증 접근 방법을 제공하며, 모든 유형에서 클라이언트 및 액세스 지점 사이에서의 통신에 동일한 802.1x 프로토콜과 프레임워크를 사용한다. 대부분 프로토콜에서 802.1x 인증 처리가 완료되면 단말에서 데이터 암호화를 위한 키를 수신한다. 802.1x 인증과 함께 클라이언트와 액세스 지점에 연결된 원격 인증 전화 접속 사용자 서비스(RADIUS) 서버 사이에서 인증 방법이 사용된다. 인증 처리에서는 무선 네트워크로 전송되지 않는 사용자 암호와 같은 인증서를 사용한다. 대부분 802.1x 유형은 사용자마다, 세션마다 동적 키를 지원하여 고정 키 보안을 강화한다. 802.1x는 확장 인증 프로토콜(EAP)로 알려진 기존 인증 프로토콜을 사용을 통해 이익을 얻는다. 무선 LAN에 대한 802.1x 인증에서 3개의 주요 구성 요소가 있다. 인증자(액세스 지점), 단말(클라이언트 소프트웨어) 및 인증 서버(원격 인증 전화 접속 사용자 서비스 서버(RADIUS)로 구성된다.

2.1.5 Virtual Private Network(VPN)

기업용 네트워크의 경우, 무선 액세스에 대한 VPN 솔루션은 현재 WEP과 MAC 애드레스 필터링에 대한 가장 적합한 대안으로 부상하고 있다. VPN은 이미 인트라넷과 리모트 액세스에 폭넓게 사용되고 있다. VPN은 데이터를 보호하고 인증된 사용자만이 네트워크에 액세스할 수 있도록 하는 다양한 업계 표준의 보안 메커니즘을 채택하고 있다. IEEE에 의해 규정된 IPSec(Internet Protocol Security)은 데이터를 암호화 하며 패킷 인증을 위해 보다 엄격한 키 알고리즘(HMAC, MD5, SHA)을 적용하며, 공개 키 인증을 위해 디지털 인증서를 사용하는데다 DES, 3DES 등을 사용한다. VPN은 또한 RADIUS, SecureID, 디지털 인증서와 같은 다양한 사용자 인증 방법을 지원한다. 이러한 표준 기반 방법을 통해 기존 네트워크 인프라에 대한 통합도 한층 용이해진다. IPSec 프로토콜에는 세 가지 주요 보안 요소가 포함되어 있다. AH(Authentication Header)의 경우 IP 데이터그램에 대한 인증 정보를 제공하며, ESP(Encapsulation Security Payload)는 비밀성을 제공한다. 또한 IKE(Internet Key Exchange)는 AH와 ESP에 채택된 암호화 알고리즘의 확장 가능한 교섭 기능을 제공한다. VPN(IPSec)과 802.11의 결합은 최근의 무선 네트워킹 보안에 이상적인 솔루션이다.



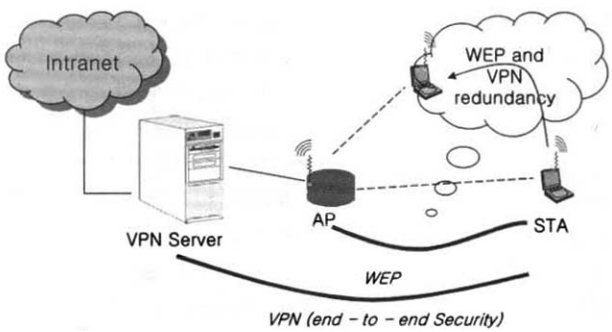
(그림 3) VPN 구조

이러한 솔루션을 통해 무선 AP는 어떠한 암호화 없이도 개방형 액세스로 구성될 수 있으며 VPN이 보안을 담당하게 된다. VPN 서버는 무선랜에 대한 캡슐화 기능과 인증 및 완벽한 암호화 기능을 제공한다. VPN 접근 방법은 인터넷을 통한 DSL/케이블 모뎀 접속이나 공항과 호텔에서의 공중 무선 AP, 구내 무선 액세스 등과 같은 다양한 방법을 통해 기업 네트워크에 접속하는 사용자들을 처리하는데 있어서의 유연성을 제공해준다[12].

2.2 인증 프로토콜의 개요

앞에서 언급한 것과 같이 VPN은 현재 IEEE 802.11 솔루션이 보안상 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 동기화를 이용해서 데이터를 인증하는 방법을 사용한다. SOLA(Statistical One-bit Lightweight Authentication)는 비용이 많이 드는 인증 기술대신 한 비트를 이용해서 인증 하는 방법을 사용한다. AP와 STA는 랜덤한 인증 스트림을 각각 가지고 있어서 이 랜덤한 값을 한 비트씩 MAC-layer를 이용해 삽입하여 스트림 값을 서로 비교하면서 인증하는 방식이다. 무선 네트워크 환경에서는 데이터를 손실하기 쉽고 또 불법 사용자가 데이터를 중간에 빼낼 수 있는데 SOLA를 적용함으로써 이런 일들을 예방할 수 있다.



(그림 4) 802.11 네트워크에서 WEP과 IPSec/VPN

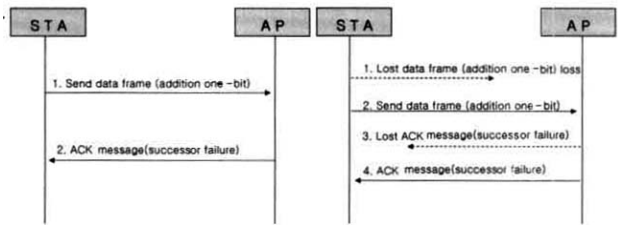
3. 제안하는 인증 프로토콜 연구

본 장에서는 WEP과 VPN 결합방식[8, 13]에서의 중복된 인증방식을 제거한 단일 비트 인증방법을 제안한다. 본 논문은 네트워크 상에서 불법 사용자 또는 여러 가지 문제로 인해 데이터를 잃었을 때 동기화하는 작업이 핵심 과제이다.

3.1 개 요

최근에 네트워크에서 전송되는 정보를 더욱 확실히 인증하기 위해 VPN과 WEP이 같이 사용되고 있다. 그러나 인증과정에서 불필요하게 중복되는 부분이 생기게 되는 문제가 있다. IPSec/VPN의 경우 인증 또는 암호화 과정 없이 Link-layer를 통과하는 문제가 발생한다. 이 문제를 해결하기 위해 IPSec/VPN은 기존 그대로 사용하고 Link-layer를 보안할 수 있는 WEP을 대체하는 인증 프로토콜을 제시한다. 여기서는 각 패킷에 한 비트만을 추가함으로써 WEP 사용으로 인한 중복되는 인증과정 제거로 전송 throughput을 향상시킬 수 있고 간편하게 전송되는 데이터를 인증하게 된다.

이 프로토콜의 주된 아이디어는 STA와 AP가 같은 인증 스트림을 가지고 있어서 데이터를 전송할 때, 인증을 위해 MAC-layer 헤더에 인증 스트림의 비트를 추가시켜 전송하면 AP에서는 AP의 인증 스트림과 전송받은 비트가 동일한지 비교하며 데이터를 인증하는 방식이다. 인증 스트림을 생성하는 것은 STA와 AP가 최초 접속을 셋업 할 때에 세션키를 서로 분배 하는 것으로 이루어진다. 이 세션키를 기초로 랜덤값을 인증 스트림에 동일하게 생성하게 된다. 다음은 STA와 AP의 인증과정을 보여준다.



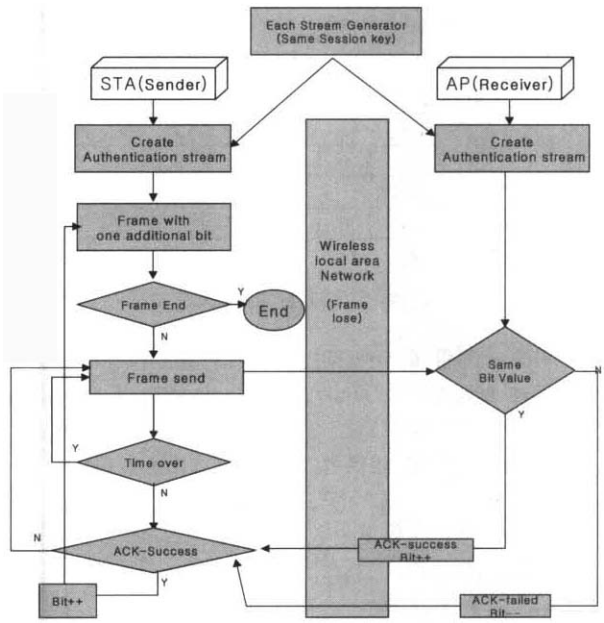
(그림 5) 왼쪽은 정상적인 인증과정, 오른쪽은 네트워크에서 에러 발생 시 인증과정

같은 세션키를 가지고 랜덤하게 만든 비트의 배열을 인증 스트림이라고 부르기로 하자. (그림 5)는 STA와 AP가 초기화된 인증 스트림을 이용해서 데이터를 전송하는 과정을 간략하게 나타낸다.

- 데이터 프레임을 성공적으로 전송할 때
  - Step 1. STA는 전송할 데이터 프레임에 인증 스트림의 한 비트를 추가하여 AP에게 전송하게 된다.
  - Step 2. STA에게 전송받은 데이터의 인증 비트와 AP 인증 스트림의 인증 비트가 동일한지 비교한 후 동일하면 STA에게 ACK-success를 전송하고 동일하지 않으면 ACK-failed를 전송함으로써 인증한다.

- 데이터 프레임 또는 ACK를 잃었을 때
  - Step 1. 데이터 프레임을 전송하였을 때 불법 사용자가 가져가거나 네트워크 오류 때문에 소실되면 STA는 이 상황을 인식하지 못하고 ACK를 기다린다.
  - Step 2. STA는 AP로부터 ACK 메시지가 전송되기를 일정시간 기다리다가 동일한 데이터 프레임을 재전송 한다.
  - Step 3. AP는 데이터를 전송받고 인증 스트림과 비교한 후 ACK를 전송한다. 그러나 ACK를 다시 네트워크 상에서 잃는다면 Step 2와 같이 STA는 데이터 프레임을 다시 전송하게 된다.
  - Step 4. AP는 재전송 된 데이터 프레임을 받고 인증 비트를 비교 후 ACK 메시지를 전송한다.

(그림 6)은 동기 알고리즘의 단계별 수행과정을 순서도를 통하여 보여준다.



(그림 6) 동기 알고리즘 흐름도

3.2 동기 알고리즘

동기 알고리즘은 인증 스트림을 동기화하기 위하여 사용된다. 기본적으로 STA와 AP는 같은 세션값으로 동일하게 만든 인증 스트림의 포인터를 움직이면서 각각의 비트를 체크하게 된다. 그러나 3.1절에서 보았듯이 STA나 AP에서 ACK를 잃었을 때 인증 스트림의 포인터가 맞지 않게 되어 문제가 생기게 된다. 일예로 AP는 ACK-success 메시지를 전송하고 인증 스트림의 포인터를 다음에 올 비트를 위해 한 비트 앞으로 움직이게 된다. 그러나 STA가 ACK-failed 메시지를 전송받거나 제한된 시간 안에 메시지를 전송받지 못하게 되면 또다시 같은 데이터 프레임을 재전송한다. 좀더 자세히 설명하자면, STA인증 스트림 포인터는 AP 인증 스트림 포인터 보다 앞에 위치할 수 없다. STA 인증 스트림 포인터 움직임 횟수는 AP의 움직임보다 적게 되고 이는 결과적으로 STA의 전력 소비를 절약할 수 있다. 이것이 제한된 전력을 가지고 있는 모바일 스테이션을 위한 중요한 요소이다. 다음은 AP와 STA에서 동기 알고리즘을 나타낸 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
```

다음은 동기 알고리즘을 분석한 결과이다.

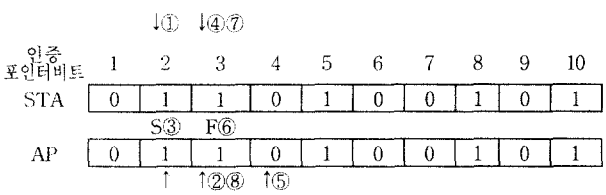
Lemma 1. STA와 AP의 동기화 할 때 STA의 인증 스트림의 포인터(Psta)는 AP의 포인터(Pap) 보다 항상 작거나 같다.

Proof : STA는 AP의 ACK-success를 전송 받아야지만 한 포인터 증가(Case i)한다. AP는 STA에게 ACK-failed를 전송 하였을 때 Case ii)와 같이 인증 포인터를 감소시킨다. AP가 전송한 ACK-success를 잃어버렸을 때 AP는 ACK를 잃어버린 상태를 인식하지 못하고 Case iii)의 여전히 증가된 상태로 있게 된다. 그 결과 AP의 포인터 값은 항상 STA의 포인터 값보다 항상 크거나 같다.

```
i)  ACK-success : Psta++, Pap++ so, Psta = Pap
ii) ACK-failed : Pap-- so, Psta = Pap
iii) AP ACK-loss : Pap++ so, Psta < Pap
```

(그림 7)에서와 같이 처음 AP와 STA 둘 다 인증 포인터 비트 2번에 있다고 가정한다.

STA에서 데이터 프레임을 AP에게 전송(①)하고 포인터는 여전히 같은 곳에 있다. AP는 데이터 프레임을 전송받고 자신의 인증값과 비교 후 동일하므로 한 포인터 증가(AP인증 포인터 비트 3번으로 증가 ②)하고 ACK-success(S③)를 STA에게 전송한다. STA는 AP에서 ACK-success가 도착했을 때 비로써 다음 포인터 ④로 증가된다. 같은 방법으로 3번 인증 포인터의 값을 AP에게 전송하고 인증값이 동일하므로 한 포인터 움직인 ⑤로 옮긴다. AP는 ACK-success ⑥을 전송하였는데 이를 잃었다고 가정할 때, STA에서는 ACK가 오지 않으므로 다시 3번 인증 포인터 ⑦을 재전송한다. 전송받은 비트를 확인한 후 AP에서는 비동기(STA bit-3은 1, AP bit-4는 0)를 확인하고 한 포인터 감소한 3번 인증 포인터 ⑧로 감소해서 동기를 맞추게 된다. 이 예제에서 제시한 바와 같이 AP의 포인터 값은 STA보다 항상 앞서거나 같은 포인터에 위치하게 된다.



S : 안전하게 STA에게 전달된 ACK F : 네트워크 상에서 ACK 잃음
①~⑧ : 인증 과정

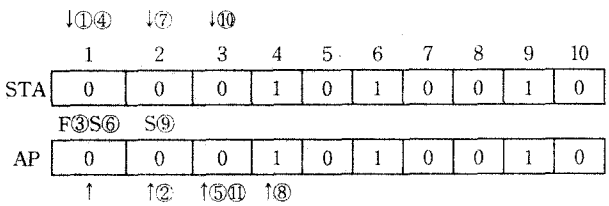
(그림 7) 동기화 과정 예제

Lemma 2. 비동기화 되었을 때 STA와 AP는 서로 다른 인증 값이 발생 할 때까지 그 사실을 인식하지 못한다.

```
i)  Psta = Pap, *Psta = *Pap
ii) Psta ≠ Pap, *Psta = *Pap
iii) Psta ≠ Pap, *Psta ≠ *Pap
```

Proof : Case i)은 포인터 주소값과 인증 값이 모두 같은 경우로 정상적인 상황이고 Case ii)는 포인터 주소값은 다르고 인증 값은 같은 경우로 동기화 되지 않아도 데이터 프레임을 계속 전송하게 된다. 마지막으로 Case iii)는 포인터의 주소값과 인증 값이 서로 틀리게 된다. 동기화 되지 않았을 때, Case iii)의 경우가 되서야 동기 알고리즘을 실행하게 된다.

예를 들어 (그림 8)의 STA는 1번 인증 포인터 비트 값을 전송하고 AP는 2번 포인터 ②로 증가하고 ACK-success ③을 보내지만 네트워크에서 잃어버린다(F③). STA는 ④를 재전송 한다. AP는 동기가 안 맞았음에도 불구하고 인증값(STA bit-1은 0, AP bit-2는 0)이 같기 때문에 ACK-success ⑥을 보낸다. 서로 다른 인증 값이 나올 때까지 비동기 상태로 AP의 인증 과정 ⑧까지 계속 진행된다. 이때 STA의 3번 포인터 ⑩을 보냈을 때 비로써 인증값이 틀린 것을 인식하고 동기를 맞추기 위해 동기화 알고리즘을 실행하게 된다.



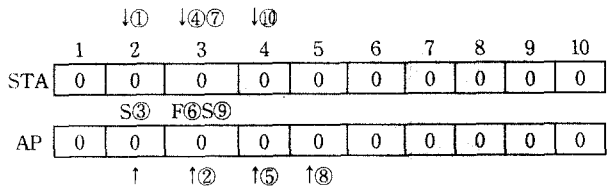
(그림 8) 동기화 과정 예제

Lemma 3. 인증 스트림의 인증 값은 0과 1의 비율에 따라 동기화 하는데 영향을 미친다.

Proof : STA와 AP는 인증 스트림의 배열 값을 만들기 위한 랜덤 함수 알고리즘을 사용한다. 랜덤 함수 알고리즘은 세션키를 이용해 0과 1을 랜덤하게 만들어 스트림을 구성하게 되는데 그 비율에 따라서 인증하는데 영향을 미치게 된다. 결과적으로 Lemma 2에서 Case ii) 발생시에 동기화를 실행하려면 Case iii)의 경우에서야 동기 알고리즘을 수행하기 때문이다.(본 논문에서는 0과 1의 비율을 50%로 가정한다.)

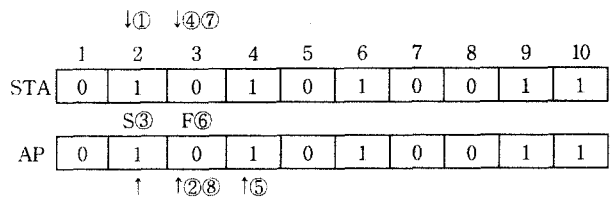
- 인증 스트림 값이 모두 동일한 경우
  - Case ii)와 같은 경우 발생시 비동기 상태를 인지하지 못하고 계속 데이터 프레임을 전송하게 된다. 즉 비동기 상태에도 다음 비트가 동일한 인증값을 가지고 있으므로 비동기 상태를 인지 할 수 없는 상황이 된다. 인증 스트림 값이 모두 동일하기 때문에 AP는 계속 ACK-success 만을 전송하기에 문제가 발생한다.

  (그림 9)는 두 번째 인증 포인터 비트까지 전송 받았다고 하고, 3번 인증 포인터 ④를 전송한 것을 AP에서 받고 한 포인터 ⑤증가시킨 후 보낸 ACK-success ⑥을 네트워크에서 잃어버린다. 일정 시간 후 STA에서는 재 전송 ⑦을 한다. 동기화 되지 않았으나 이를 인식하지 못하고 다음 포인터 ⑧로 옮기고 ACK-success(S⑨)를 보낸다. 결과적으로 비동기 상태로 계속 데이터 전송은 진행된다.



(그림 9) 동기화 과정 예제

- 인증 스트림 값 0과 1의 비율이 50%일 때
  - 0과 1의 비율이 50%일 때 비동기 상태 일 때라도 다음 비트가 서로 다른 인증값이 올 확률이 50%이므로 비동기 상태를 바로 인식하고 동기화하게 된다.



(그림 10) 동기화 과정 예제

4. 성능 평가 및 분석

데이터를 전송받는 사용자는 전송하는 사용자가 인가된 사용자인지 비인가 된 사용자인지 모르고 데이터를 전송 받게 된다. 즉 AP는 STA의 인가여부를 알 수 없다. 따라서 이 장에서는 데이터를 전송한 사용자의 인가여부를 확률적으로 분석하고, 시뮬레이션을 통해 본 논문에서 제안한 동기 알고리즘과 기존 알고리즘을 비교 분석한다.

AP는 동기 알고리즘의 수행 정도를 측정하여 STA의 정상 여부를 확인할 수 있게 된다. 이 제안한 확률은 단일 Bit를 사용하는 동기 알고리즘(Wang's scheme[5])의 수식과 비슷하지만 인증 방법상 제안한 방법과 더 적합하기에 기술한다.

인가되지 않은 사용자가 인증 스트림의 n-비트를 모두 알아낼 확률은 2^{-n}이다. 이것은 각각의 인증 스트림은 0과 1로 구성되어있고 둘 중 하나를 알아낼 확률이 1/2이기 때문이다. 인가된 사용자이거나 비인가 된 사용자인 STA가 데이터를 보낼 확률을 각각 50%라고 가정한다. P(illegal user)=50%, P(legal user)=50%. 이 확률은 연속해서 ACK-loss가 일어나지 않는다는 전제로 Bayes' 정의와 binomial 분포를 이용한다. 다음 예는 인증 스트림의 길이는 N, 인증과정 중 ACK-loss로 인한 동기 알고리즘 수행 횟수를 n, 이미 알고 있는 ACK-loss 확률은 p라고 한다. P(S=legal user | N, n)는 인가된 사용자가 데이터를 보낸 확률이다. Bayes' 정의를 이용하면,

$$P(STA = legal\ user|N, n) = 1 - P(STA = illegal\ user|N, n) \quad (1)$$
$$= \frac{P(N, n|STA = legal\ user)}{P(N, n|(STA = legal\ user) + P(N, n|(STA = illegal\ user)}$$

(1)과 같은 식이 되고 이 식을 유도하기 위한 각각의 확률적 계산방법은 다음과 같다. 인가되지 않은 사용자는 인증 스트림을 알지 못하여 다음 비트 값을 0과 1중 추측할 수밖에 없다. 그렇기 때문에 (2)와 같은 수식에 성공할 확률 2^{-N}만 적용한다. 그래서 (2)와 같은 식이 산출된다.

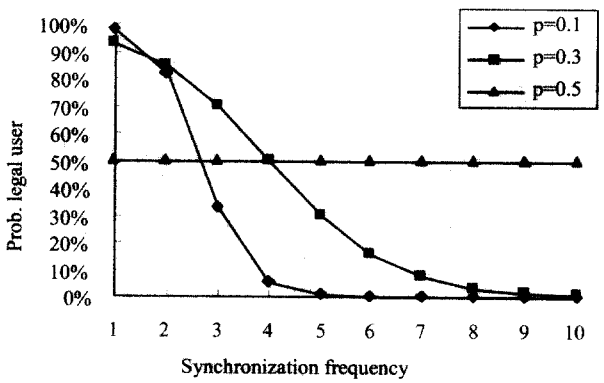
$$P(N, n|STA = illegal\ user) = \binom{N}{n} * 2^{-N} \quad (2)$$

$$P(N, n|STA = legal\ user) = \binom{N}{n} * p^n(1-p)^{N-n} \quad (3)$$

(2)와 (3)을 결합해서 (1)과 같은 식을 도출해 낼 수 있다. 이와 같은 방법으로 (4), (5)와 같은 인가된 사용자와 비인가된 사용자가 데이터를 보낸 확률을 구할 수 있다.

$$P(STA = legal\ user|N, n) = \frac{p^n(1-p)^{N-n}}{2^{-N} + p^n(1-p)^{N-n}} \quad (4)$$

$$P(STA = illegal\ user|N, n) = \frac{2^{-N}}{2^{-N} + p^n(1-p)^{N-n}} \quad (5)$$

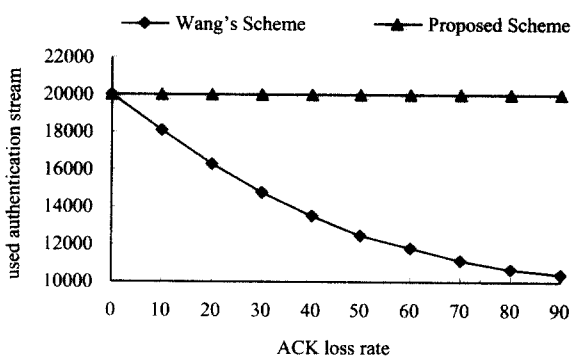


(그림 11) n번 동기 알고리즘을 수행했을 때 인가된 사용자일 확률(N=10)

(그림 11)은 동기화 알고리즘 수행 결과로 제시한 수식을 통해 데이터를 전송한 사용자의 인가 여부를 확인할 수 있다. 반대로 확률값을 통해 공격자일 확률을 검출 가능하다. p는 0.1, 0.3, 0.5로 각각 적용하고 N은 10이라고 가정한다. 예를 들어 10개의 인증 스트림을 사용하면서 동기 알고리즘을 4번(n=4) 수행했고 ACK-loss 확률이 0.3일 경우 STA가 인가된 사용자일 확률은 0.493이다. 그러므로 비인가 된 사용자일 확률은 0.507(1-0.493)이다. 앞에서 언급했듯이 이 수식이 제안한 스킴에 더 적합한 이유는 Wang's 방법의 경우 연속된 ACK-loss가 없는 경우에 한에서 10개의 인증 스트림이 있을 때 최대 다섯 번 동기 알고리즘을 수행하면 인증 스트림을 모두 사용하기 때문에 스트림을 재 할당해야 한다. 반면 제안한 스킴의 경우 같은 조건하에 인증 스트림 개수만큼 동기 알고리즘을 수행(10회)할 수 있기 때문에 더 인증 스트림을 효율적으로 사용하게 된다.

다음은 제시한 동기 알고리즘과 기존 Wang's 알고리즘을 C 언어를 사용하여 시뮬레이션 한 결과를 토대로 성능평가 및 비교 분석 한다. Wang's 방식과 본 논문에서 제시한 방식과의 가장 큰 차이점은 동기를 위한 포인터 위치 교정이 AP에서 일어난다는 것이다. 시뮬레이션은 20,000bit의 인증 스트림을 10번 수행한 결과 평균을 도출한 값이다.

(그림 12)는 우리의 인증 방식과 Wang's 인증 방식에서 ACK-loss의 확률에 따라 20,000bit의 인증 스트림의 사용 정도를 보여준다. Wang's 방식은 ACK-loss 확률이 커감에 따라 눈에 띄게 인증 스트림 이용 정도가 감소한다. 이와 비교하여 제시한 인증 방법은 항상 인증 스트림을 100% 이용률을 보여준다. 실제로는 ACK를 잃을 확률이 30%~90%까지 높게 나타나지는 않지만 비교 평가를 위해 넓은 범위의 에러율을 적용한 것이다. 그림에서 보이는바와 같이 기존에 제안된 Wang's 방식보다 우리 방식에서 더 효과적으로 인증 스트림이 활용된다. WEP에서의 문제점 중 IV(Initialization Vector)를 모두 다 사용하였을 경우에 재 할당해야 하는 문제가 있는데 여기서 제안하는 프로토콜은 인증 스트림을 재 할당하는데 시간도 적게 걸릴 뿐만 아니라 기존에 있던 방식보다 효율적으로 스트림을 사용하는 것을 볼 수 있다. 예를 들어 ACK-loss 확률이 20%일 때 제안한 방식은 20,000bit의 인증 스트림을 모두 사용하는데 반해 Wang's 방식은 16,000bit 인증 스트림을 사용하면 스트림을 재 할당해야 한다. 인증 스트림은 일단 모두 사용하게 되면 재 할당 시 시간을 소모 하게 된다. 그러므로 제안한 인증 방식은 효율적인 인증 스트림 사용으로 시간을 단축시킬 수 있다. 또한 이 새로운 인증 프로토콜은 기존 802.11에서 어떤 변화 없이 간단히 추가시키는 것만으로 효과를 볼 수 있는 특징을 가지고 있다.



(그림 12) ACK를 잃었을 때의 인증 스트림 사용

5. 결론 및 향후 연구

본 논문에서는 IEEE 802.11 네트워크 접속 시 효과적인 인증 프로토콜에 대하여 제안하였다. 이 프로토콜은 두 스테이션 사이에 단지 한 비트만을 사용해 인증을 할 수 있고 기존의 방식보다 더 효율적인 성능을 확인하였다. 새로운

동기화 알고리즘을 이용하여 최대 50%까지 인증 스트림을 효율적으로 사용할 수 있다는 것을 시뮬레이션을 통해 검증하였고, 또한, AP측에서 동기화 과정을 수행하기 때문에 모바일 스테이션 측에서의 전력소모를 최소화 할 수 있는 장점도 확보하게 되었다.

본 연구는 무선 통신에서 새로운 인증 프로토콜을 위한 토대로 제시하였다. 본 논문의 인증 프로토콜은 무선 환경에서의 보안 통신을 제공 시 매우 유용하게 이용될 수 있을 것이다. 많은 조직이나 기업체가 무선 환경을 이용하면서 강화된 보안 정책의 필요성을 느끼고 있다. 향후 해커의 공격에 대한 보안, 로밍 지원을 위한 지원, 부적절한 AP의 활용 및 서로가 인증하는 사용자가 아닌 사용자에 대한 관리 점검, 무선 사용자의 전반적인 관리 등의 보안 개발 및 연구가 추가로 필요하겠다.

참 고 문 헌

[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 internet 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.

[6] http://neocisco.metabrain.com.

[7] http://www.datanet.co.kr.

[8] N. Borisov, I. Goldberg and D. Wangner, "Interception Mobile Communications : The Insecurity of 802.11".

[9] Yanyan Yang, Zhi Fu, Wu, S. F., "Bands : an inter-domain internet security policy management system for IPSec/VPN," Integrated Network Management, IFIP/IEEE Eighth International Symposium on, 2003.

[10] Bhagavathula R., Thanthry N., Pendse R., "Mobile IP and virtual private networks," Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th Sept., 2002.

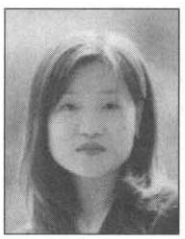
[11] CREWAVE CO., Ltd, available from http://www.crewave.com/Korean/menu/support/tech/tech_1.htm.

[12] Jingdi Zeng, Ansari, N., "Toward IP virtual private network quality of service : a service provider perspective," Communications Magazine, IEEE, Vol.41, Issue.4, April, 2003.

[13] Intel, "VPN and WEP Wireless 802.11b security in a corporate environment," Intel white paper, March, 2003.

[14] http://support.jp.dell.com.

조 혜 숙



e-mail : jojo@skku.edu

2003년 한성대학교 정보전산학부(학사)

2003년~현재 성균관대학교 컴퓨터공학과 (석사과정)

관심분야 : 모바일 컴퓨팅, 모바일 인증, 정보보안

윤 희 용

e-mail : youn@ece.skku.ac.kr

1977년 서울대학교 전기공학과(학사)

1979년 서울대학교 전기공학과(석사)

1988년 Univ. of Massachusetts 컴퓨터공학과(박사)

1988년~1991년 Univ. of North Texas. 조교수

1991년~1999년 Univ. of Texas at Arlington 부교수

1999년~2000년 한국정보통신대학교 교수

2000년~현재 성균관대학교 정보통신공학부 교수

관심분야 : 모바일 컴퓨팅, 분산처리, 시스템 소프트웨어