제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

# WPA TKIP 알고리즘의 소프트웨어 구현과 하드웨어 구현의 액세스포인트 성능 비교

오경희, 강유성, 정병호
한국전자통신연구원 무선인터넷보안연구팀
e-mail : khoh@etri.re.kr

# Performance Evaluation between Software Implementation and Hardware Implementation of WPA TKIP Algorithm in Access Points

Kyunghee Oh, Yousung Kang, Byungho Chung
Wireless Internet Security Research Team, ETRI

요 약

IEEE 802.11 표준에 포함되어 있는 WEP 방식의 무선랜 보안이 취약한 것으로 알려진 후, WEP을 대치할 새로운 표준이 802.11i 워킹그룹에 의하여 작성되고 있으며, Wi-Fi는 중간단계로서 802.11i의 일부만을 구현하는 WPA 규격을 만들었다. WPA 규격 중 TKIP 알고리즘을 디바이스 드라이버에 소프트웨어로 구현한 액세스포인트와 펌웨어에 구현한 액세스포인트를 개발하여, 시험을 통하여 성능을 비교 분석하였다.

## 1. 서론

IEEE 802.11 표준[1]을 따르는 무선랜은 기업의 사설망, 핫스팟과 같은 공중망, 그리고 일반 가정과 소규모 사업장에서도 사용하는 등 사용자가 계속 늘어나고 있다. 그런데, 기존의 무선랜 제품이 사용하여온 WEP 방식에 의한 보안에 취약점이 있음이 알려졌고[2], 이를 해결하는 새로운 보안 표준이 IEEE 802.11i 워킹그룹에 의하여 작성되고 있다[3].

그러나, 표준의 승인이 지연되면서, 무선랜 관련 업체들의 연합체인 Wi-Fi 에서 IEEE 802.11i 규격이 완성되기 이전의 중간단계로서 WPA 규격[4]을 발표하여 실제 무선랜 제품 개발에 사용하고 있다. WPA 규격에서는 기존의 무선랜 하드웨어에서 소프트웨어 및 펌웨어만을 수정함으로써 IEEE 802.11i 규격의 일부를 준수할 수 있게 한다.

본 논문은 리눅스 환경에 구현된 기존의 무선랜 액세스포인트 시스템을 기반으로, WPA 규격을 준수하도록 구현한 시스템에 대하여 논의한다. 기존의 액세스포인트 디바이스 드라이버를 수정하여 TKIP 암호 알고리즘을 디바이스 드라이버 내부에 구현한 시스템과 무선랜 하드웨어 내부의 펌웨어에서 TKIP 암호 알고리즘이 구현된 액세스포인트를 각각 구현하고, 시험을 통하여 이에 대한 성능을 비교 분석하였다.

## 2. WPA 규격

WPA 규격은 IEEE 802.11i draft 3.0 에서 하드웨어 수정 없이 구현하기 힘든 CCMP 암호 알고리즘을 제외한 나머지 부분을 기반으로 실제 구현과정에서 발견된 몇 가지 오류를 수정한 내용으로 구성된다.

### 2.1 인증 및 키 교환

사용자 인증 방법은 IEEE 802.1x[5]을 따르는 방식과 PSK 방식이 있다.

IEEE 802.1x 에는 역할에 따라 세 가지 시스템이 있다. 서비스를 제공하고자 하는 포트에 대하여 인증을 수행하는 authenticator, authenticator 에서 제공하는 포트의 인증을 받고자 하는 supplicant, supplicant 의 신분을 인증하여 authenticator 가 서비스를 제공할 수 있도록 알려주는 authentication server 로 구성된다. authenticator 는 supplicant 와 주고받는 EAPOL 프레임으로 supplicant 와 authentication server 사이의 EAP 메시지를

중계하여 인증과정을 수행한다. 그리고 인증에 성공한 supplicant 들에 대해서만 망으로의 데이터 프레임 전송을 허용한다. WPA 에서는 액세스포인트가 authenticator 의 역할을 수행하며, 인증이 완료된 후 액세스포인트와 스테이션 사이에 공유키가 생성된다.

기업망이나 공중망과는 달리, 소호 및 홈네트워크에서는 굳이 별도의 인증 서버를 둘 필요가 없다. 이러한 환경에서는 액세스포인터와 스테이션에 미리 공유키를 설정해 두는 PSK 방식을 사용할 수 있다.

액세스포인트와 스테이션은 공유키를 사용해 실제 데이터 프레임의 암호화에 사용되는 임시키를 생성하기 위한 키교환 과정을 수행하며, 각각의 스테이션이 할당되는 pairwise 키와 여러 스테이션이 공유하는 group 키를 생성한다. 이때의 키교환 과정에서 IEEE 802.1x 에서 지정한 것과는 다른 IEEE 802.11i 에서 지정한 키 프레임 형과 키 교환 절차에 따른다.

### 2.2 TKIP

암호알고리즘으로는 TKIP 과 기존의 WEP 을 사용할 수 있다. IEEE 802.11i 표준에서 필수사항인 CCMP 알고리즘의 구현이 WPA 규격에서는 선택사항이다.

CCMP 가 AES 알고리즘을 사용하는 것과는 달리, TKIP 은 WEP 을 확장하는 방법을 사용함으로써, 기존의 하드웨어 교체가 필요 없이 구현할 수 있도록 설계되었다.

그림 1 과 그림 2 는 각각 TKIP 알고리즘의 암호화 및 복호화 과정을 보여준다. Temporal 키와 MIC 키는 스테이션의 인증과정에서 생성된 키 값으로, 스테이션이 액세스포인트에 인증 받을 때마다 새로운 값이 설정된다. Temporal 키 값과, 각 데이터 프레임마다 1 씩 증가하는 카운터인 TSC 로부터, key mixing 과정을 거치면 WEP 에 사용되는 seed 가 생성된다. 이 seed 는 전송되는 각 데이터 프레임마다 매번 다른 값을 가지게 된다. 또한, MIC 키를 사용하여 메시지 인증코드 MIC 를 프레임에 포함시킨다. 이러한 과정을 거쳐 암호화된 데이터 프레임은 알려진 WEP 알고리즘의 취약점으로부터 안전하게 된다.

복호화 과정에서 프레임 헤더의 IV 필드에 포함된 TSC 값과 이전에 수신한 TSC 값을 비교 확인하여, 재전송에 의한 공격을 방지한다. 그리고, MIC 인증코드의 확인을 통하여 데이터 무결성을 검증한다.

### 2.3 IEEE 802.11i 와 다른 점

아직 완성된 표준이 아닌 IEEE 802.11i draft 3.0 을 실제 제품으로 구현하는 것에는 문제점들이 있어, WPA 규격에서는 TKIP 방식을 사용하는 것 이외에 IEEE 802.11i 내용 중 일부를 좀더 수정하였다.

WPA 에서는 향후 표준화가 완성된 후에 사용될 RSN Information Element 와 구분하기 위하여, 별도의 WPA Information Element 를 management 프레임에서 사용한다. 그리고, 기존의 WEP 을 사용하는 스테이션을 함께 사용할 수 있는 mixed-mode 를 구현할 수 있다. 이외에도 draft 내의 오류로 보이는 사항들이 수정되었다.

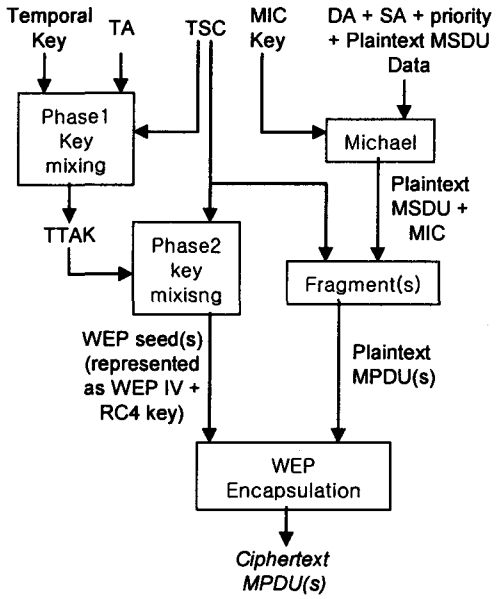


그림 1. TKIP 암호화 과정

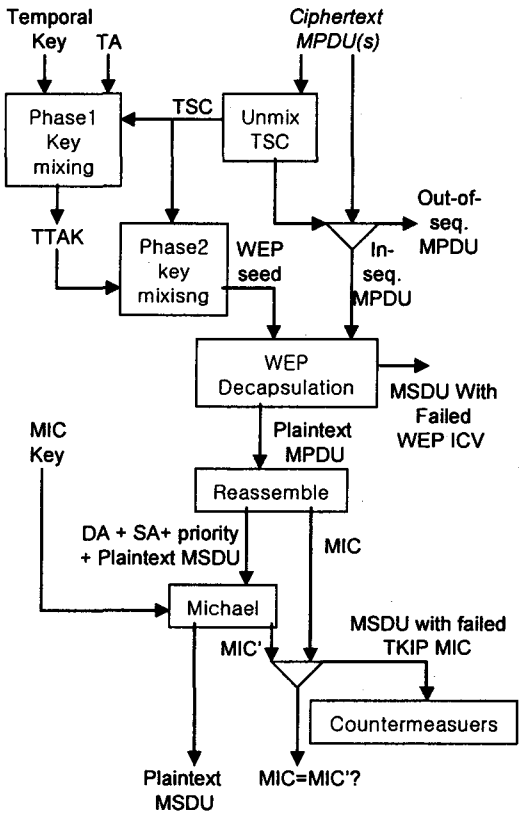


그림 2. TKIP 복호화 과정

### 3. 액세스포인트의 구현

WPA 를 지원하는 무선랜 액세스포인트는 스테이션 인증과정을 담당하는 응용과 디바이스 드라이버, 무선랜 카드로 구성된다. TKIP 알고리즘을 디바이스 드라이버에 구현한 시스템과 무선랜 카드의 펌웨어에 구현된 시스템을 각각 개발하였다.

두 시스템 모두 운영체제로 리눅스 커널 2.4 를 사용하였다. 인증과정을 담당하는 응용은 두 시스템에서 동일하며, TKIP 을 구현 위치에 따라 디바이스 드라이버와 사용된 무선랜 하드웨어가 다르다. 디바이스 드라이버는 Prism 계열의 MAC 칩을 사용하는 무선랜 장비에 대한 소스코드가 공개되어 있는 리눅스용 액세스포인트 디바이스 드라이버인 HostAP 디바이스 드라이버[6]를 수정하여 사용하였다.

그림 3 과 그림 4 는 각각 소프트웨어 및 하드웨어 방식에 의한 TKIP 구현 액세스포인트의 기능 블록 구성을 보여준다.

소프트웨어 방식에 의한 구현은 디바이스 드라이버에 TKIP 알고리즘을 구현하기 위하여 HostAP 디바이스 드라이버에 TKIP 알고리즘을 추가하였으며, 스테이션용 무선랜 하드웨어를 사용하였다. 이 방식을 사용하면 디바이스 드라이버에서 데이터 프레임에 대하여 모든 암호화 과정을 수행한 후에 하드웨어로 데이터 프레임을 보낸다.

하드웨어 방식에 의한 구현은 WPA 가 지원되는 액세스포인터용 무선랜 하드웨어를 사용하였다. 이 방식에서는 하드웨어에 Temporal 키와 MIC 키를 미리 설정해 두고, 암호화 되지 않은 데이터 프레임을 하드웨어로 보내면, 하드웨어 내의 펌웨어에서 암호화를 수행한다.

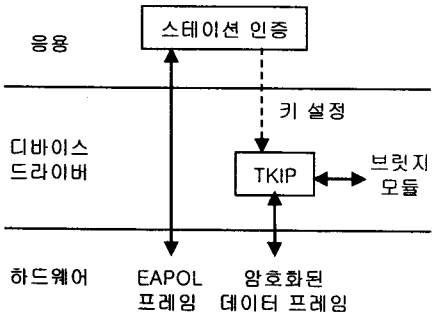


그림 3. 소프트웨어 방식의 WPA 액세스포인트

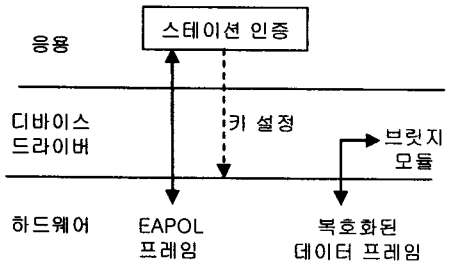


그림 4. 하드웨어 방식의 WPA 액세스포인트

액세스포인트의 개발 플랫폼으로 펜티엄 III 650MHz 데스크탑 컴퓨터와 MPC850 마이크로 프로세서를 사용한 임베디드 시스템을 사용하였다. 시험을 위한 스테이션으로는 리눅스를 운영체제로 하는 펜티엄 III 933MHz 노트북 컴퓨터를 사용하였으며, 소프트웨어 방식으로 TKIP 을 구현한 디바이스 드라이버와 WPA 인증을 수행할 수 있도록 수정된 Xsupplicant[7]를 사용하였다.

### 4. 성능 비교

성능 시험을 위하여 스테이션, 액세스포인트, FTP 서버 세 시스템을 그림 5 와 그림 6 과 같이 구성하였다. 각각 데스크탑과 임베디드 시스템을 사용하여 액세스포인트를 구현한 시험망이며, 각 시험망에 소프트웨어 방식과 하드웨어 방식에 의한 TKIP 암복호화 성능 시험을 각각 수행하였다.

성능 비교를 위하여 3.4Mbyte 크기의 파일을 FTP 서버로부터 스테이션이 받아오는 전송속도를 세 번씩 측정하였다. 성능 시험 결과는 표 1 및 표 2 와 같다.

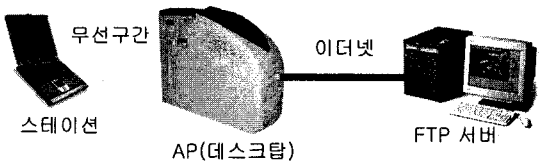


그림 5. 데스크탑 WPA 액세스포인트 시험망

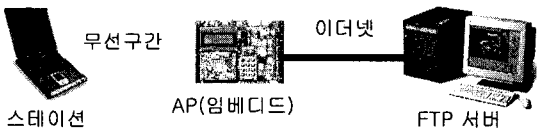


그림 6. 임베디드 시스템 WPA 액세스포인트 시험망

표 1. 데스크탑 액세스포인트 전송 속도 (단위 kByte/s)

| | 1 회 | 2 회 | 3 회 | 평균 |
|---|---|---|---|---|
| 비보안 | 462.1 | 452.2 | 440.2 | 451.5 |
| 소프트웨어 방식 | 327.3 | 303.4 | 308.8 | 313.2 |
| 하드웨어 방식 | 209.1 | 198.1 | 197.2 | 201.5 |

표 2. 임베디드 액세스포인트 전송 속도 (단위 kByte/s)

| | 1 회 | 2 회 | 3 회 | 평균 |
|---|---|---|---|---|
| 소프트웨어 방식 | 16.6 | 16.5 | 16.5 | 16.5 |
| 하드웨어 방식 | 194.6 | 183.1 | 181.4 | 186.4 |

TKIP 등의 암호알고리즘 보안을 적용하지 않은 표 1 의 비보안 시험에서 파일 전송속도는 451.5kByte/s 가 측정되었다. 이 값은 IEEE 802.11b 하드웨어의 대역폭 11Mbps 에서 제어 프레임과 데이터 프레임의 헤더부분으로 인한 오버헤드를 고려했을 때의 최대 전송속도와 큰 차이가 없다. 같은 환경에서 소프트웨어 방식과 하드웨어 방식을 사용하였을 때, 전송속도 성능은 각각 비보안의 69.4%, 44.6%이다. 소프트웨어 방식이 다소 성능이 우수한데, 이는 무선랜카드 내의 하

드웨어에서 암호화를 처리하는 것 보다, CPU 성능이 더 우수한 데스크탑에서 암호화를 처리하는 것이 전체의 성능 향상에 도움이 되는 것을 보여준다.

그런데, 성능이 떨어지는 CPU 를 사용한 임베디드 시스템에서는 하드웨어 방식의 전송속도가 데스크탑의 92.5%로 성능 저하의 크기가 작은 반면, 소프트웨어 방식에서는 데스크탑의 5.3%에 불과하여 현격한 성능 저하가 나타났다. 이는 성능이 떨어지는 임베디드 시스템의 CPU 로는 TKIP 암복호화 과정의 계산량을 충분히 처리할 수 없음을 나타내는 것이다.

## 5. 결론 및 향후 과제

Wi-Fi 에서 제정한 WPA 규격을 준수한 무선랜 보안기술을 통하여 사용자 인증, 접근제어, 권한 검증, 데이터 기밀성과 무결성 등의 보안 요소를 만족 시킬 수 있다[8]. 이로써, 기존의 공중 무선랜 망 또는 사설 무선랜 망에서 문제가 제기되어온 보안 결함을 해결할 수 있다.

개발된 액세스포인트는 리눅스 환경을 사용하여 제작되었으며, 데스크탑 및 임베디드 시스템 환경으로 만들어져 시험되었다. 그리고, 별도의 액세스포인트용 하드웨어를 사용하지 않고 일반 무선랜 카드에 디바이스 드라이버의 변경을 통하여 소프트웨어로 구현 방법과 WPA TKIP 을 지원하는 액세스포인트용 하드웨어 장비를 사용한 방법이 모두 구현되었다. 소프트웨어 방식의 경우, 데이터 프레임의 암호화 및 복호화 과정이 디바이스 드라이버에서 이루어지므로, CPU 의 성능에 많은 영향을 받는다. 시험을 통하여 일반 데스크탑 수준의 CPU 를 사용한다면, 오히려 WPA TKIP 이 무선랜 하드웨어로 구현된 경우보다 암호화 과정이 더 빨리 수행되어 성능이 뛰어남을 확인하였다. 그러나, 성능이 떨어지는 CPU 를 사용하면, 현저한 성능 저하가 나타났다. 이에 비해 하드웨어 방식의 경우, 많은 계산과정을 필요로 하는 암호화 과정이 CPU 가 아닌 무선랜 하드웨어에서 이루어져, CPU 성능에 따른 전송속도의 저하가 미미하였다.

암호알고리즘을 소프트웨어로 구현한 방식과 하드웨어로 구현한 방식에는 각각 장단점이 있다. 하드웨어에 WPA TKIP 을 구현하기 위해서는 제품은 무선랜 하드웨어 제품을 재구성하여야 하는 비용이 필요하지만, 소프트웨어 방식에서는 디바이스 드라이버의 교체만으로 가능하다. 그러나, 소프트웨어 방식을 사용한 임베디드 시스템의 경우, 보다 우수한 성능을 가진 CPU 를 필요로 한다.

IEEE 802.11i 표준이 확정되면, WPA 보다 강력한 RSN(Robust Security Network)이란 이름으로 무선랜의 보안이 이루어 질 것이다. RSN 과 WPA 의 가장 큰 차이점은 CCMP 알고리즘을 기본으로 사용한다는 점이다. CCMP 를 구현하기 위해서는 기존 장비의 펌웨어만을 갱신하는 것으로는 구현하기가 어려우며 새로운 하드웨어를 사용하여야 하는 것으로 알려져 있다. 그러나, CCMP 를 디바이스 드라이버 내에서 구현한다면 하드웨어 변경 없이 소프트웨어로 RSN 기능을 구현할 수 있다. 단, 이러한 방법에는 여전히 CPU 에 따른 성능 문제가 남아있다.

## 참고문헌


[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Std 802.11-1997, June 1997.

[2] W. A. Arbaugh, et al. "802.11 Security Vulnerabilities," http://www.cs.umd.edu/~waa/wireless.html.

[3] "Wireless Medium Access Contro(MAC) and Physical Layer(PHY) Specifications: Specification for Enhanced Security, " IEEE Draft 802.11i/D3.0, November 2002.

[4] "Wi-Fi Protected Access," version 2.0, Wi-Fi Alliance, April 2003.

[5] "Port-Based Network Access Control," IEEE Std 802.1x - 2001, June 2001.

[6] "Host AP driver for Intersil Prism2/2.5/3," http://hostap.epitest.fi/.

[7] "Open Source Implementation of IEEE 802.1X," http://www.open1x.org/.

[8] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화 동향 및 전망", 전자통신동향분석, 제 18 권 제 4 호, 2003 년 8 월.