유무선 네트워크 상에서 WPA 성능 분석

*설정환, 이기영
인천대학교 정보통신공학과
e-mail : aknari@naver.com, kylee@incheon.ac.kr

Performance Analysis of WPA(Wi-Fi Protected Access Technology) in Wired and Wireless Network

*Jeong-Hwan Seol, KiYoung Lee
School of Information and Telecommunication Engineering
University of Incheon

Abstract

WPA is a security service that greatly increases data protection and access control on WLANs. WPA uses TKIP that is secure algorithm of 802.11i and 802.1X/EAP authentication. It provides enhanced secure ability with the dynamic security key to correct WEP's weaknesses. In this paper, we obtain measured data transmission time that by how to create secure key of WPA in the wired and wireless network. The result shows that the delay of data transmission time was not long even if used WPA.

I. 서론

많은 조직체들은 자신들의 LAN을 인터넷에 연결하고 그들의 고객과의 통신지원, 업무의 비용절약, 업무의 자동화를 위한 방법으로 인터넷에 근거한 서비스를 사용한다[1]. 그러므로 인터넷 사용으로 인한 외부로부터의 공격에 대처하기 위한 보안 요구사항은 필수적이다. 또한 무선 통신을 이용하여 인터넷을 사용하는 사용자가 증가하면서 무선 보안에 대한 관심은 더욱 커지고 있다. 보안 서비스를 사용함에 있어서 가장 중요한 부분은 효율성이다[2]. 즉, 사용자는 안전한 시스템을 구성하면서 동시에 빠른 속도를 보장받기를 원하는 것이다. 최근의 무선 보안에 대한 요구 사항은 강력한 보안성이다. 기존의 802.11b에서의 보안 구조는 WEP을 이용한 보안 서비스의 제공이었다. 하지만 WEP의 구조적 취약성과 고정 암호키 방식으로 인한 해킹의 우려로 인해 802.11i에서는 AES를 이용한 데이터 암호화를 통해 더욱 강력한 보안 구조를 제안하였다. 하지만 현재 대부분의 하드웨어를 교체해야만 하는 문제로 인해서 개발과정이 길고, 기존의 무선 랜 카드 및 AP에 backward compatibility를 보장 못하는 문제가 있다[3]. 따라서, 소프트웨어를 통한 업그레이드로 WEP의 보안 문제점을 개선한 방법인 WPA가 그 대안으로 사용되고 있다. WPA는 고정 암호키 분배 방식의 WEP과 달리 동적 암호키 분배를 통해 향상된 데이터 보안 기능을 제공한다[4].

본 논문에서는 Ⅱ장에서 WPA의 보안 기능 및 향후 발전 과정에 대해서 살펴보고, Ⅲ장에서 실험 환경 및 유무선 네트워크 상에서 WPA의 암호키 설정 방법에 따른 데이터 전송 시간을 측정, 보안 서비스가 제공되지 않는 네트워크와의 비교를 통해 WPA의 효율성을 분석하였다. 마지막으로 Ⅳ장에서는 실험 결과 및 향후 연구 과제에 대해서 기술하였다.

본 논문은 산업자원부,한국산업기술평가원 지정 인천대학교멀티미디어 연구센터의 지원에 의한 것입니다.

II. 관련 연구

2.1 WEP 문제점

기존의 WEP은 무선랜 데이터 스트림의 보안성을 제공하기 위하여 정의한 데이터 스킴이다. WEP은 데이터 암호화와 복호화에 동일한 키, 동일한 알고리즘을 사용하는 스트림 암호 방식을 사용한다. 모든 단말은 40비트의 암호키를 공유한다(WEP2는 128비트). 단말은 40비트 암호키와 IV(Initialization Vector)를 결합, 의사 난수 키 스트림을 생성하여 평문을 암호화하여 전송한다. 액세스 포인트는 이를 복호화 하여 단말을 인증한다[5].

WEP은 IV의 크기가 작아서 실시간 공격에 약하며, 암호키는 AP에 연결된 모든 단말이 공유하므로 암호학적으로 취약하다. 그림 1은 WEP의 암호화 방식의 블록도이다.

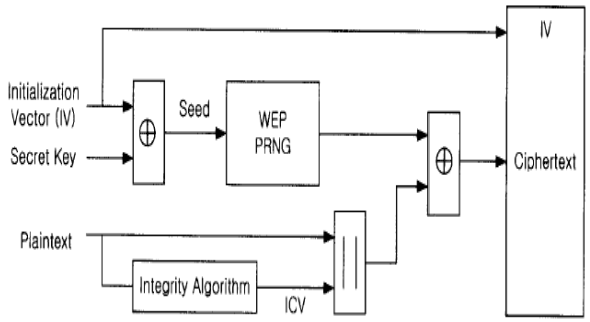

그림 2. WEP의 암호화 방식

2.2 WPA 개요

IEEE에서는 대표적인 보안 표준으로 MAC레이어에서 무선 단말과 액세스포인트 간의 장비 인증 및 데이터의 암호화를 담당하는 802.11i와 MAC레이어 상위에서 사용자 인증을 제공하는 802.1X를 발표하였다. 802.11i 태스크그룹은 무선 LAN 인프라망과 Ad-hoc 망에 적용할 수 있는 새로운 형태의 보안 아키텍처(RSN)를 제안하였다. 802.11i에서는 기존의 WEP 방식의 보안 문제점을 해결하기 위해 보다 강도 높은 알고리즘(AES)을 사용해야 하지만 MAC의 하드웨어 칩을 변경해야 하는 어려움이 있다. 그래서, 다른 관점에서 보안 문제점을 소프트웨어적으로 개선하는 TKIP 방식을 제안하고 있다. WPA는 802.1X의 인증 서비스와 802.11i의 데이터 암호화 알고리즘인 TKIP를 모두 제공하는 무선 보안 서비스이다[6]. 그림 2는 WPA가 802.11i와 거의 동일한 구조로 실행됨을 보여준다.

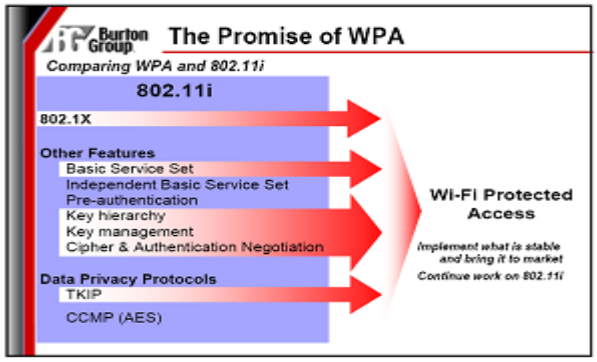

그림 1. WPA와 802.11i

2.3 WPA 특징

기존에 쓰이던 WEP 프로토콜은 키 스트림의 단순성, 도청에 의한 평문 노출, DOS 공격 가능성, 동적 키 분배 방법의 부재 및 인증 방법의 부재로 인해 보안에 큰 위험이 있음이 알려졌다. WPA 프로토콜은 크게 향상된 데이터 암호화 프로토콜(TKIP)의 사용과 함께 802.11X/EAP 인증 방법을 제공함으로써 향상된 보안 서비스를 제공한다. 표 1에서 WEP과 WPA의 암호화 및 인증 방식에 대해 비교를 하였다.

표 1. WEP와 WPA 비교

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

2.3.1 암호화

그림 3의 TKIP 프로토콜의 특징은 다음과 같다.

① 암호화 키

WEP의 40bits 암호화 키를 128bits로 증가하였다.

② 동적 키 생성

WEP의 고정키와 달리 유저, 세션 및 패킷 키마다 동적으로 생성되는 키를 사용, 인증 서버에 의해 분배되도록 하였다.

③ 계층 키와 키 관리 방법

TKIP는 순서 규칙이 있는 48비트 IV를 이용하여 키 재사용 및 재생 공격을 방지해 준다. 또한 패킷당 키

혼합 기능과, 패킷 위조 공격을 막아주는 암호 체크섬 기능이 있다.

④ WEP의 CRC-32를 이용한 메시지 인증방식의 문제점을 해결하기 위해 64비트 MIC키를 사용, Micheal 함수를 사용하여 인증코드를 생성한다[4].

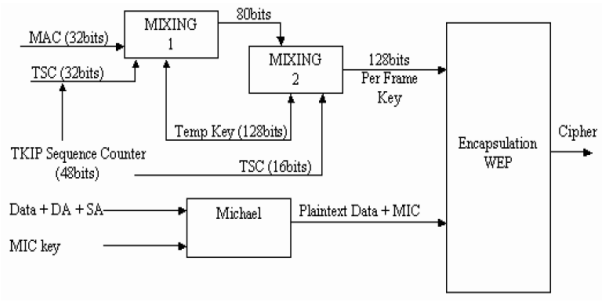

그림 3. TKIP의 암호화 방식

2.3.2 인증

WPA는 EAP(Extensible Authentication Protocol)를[1] 표준 프로토콜로 사용하는 802.1X의 인증 방법을 사용한다. EAP는 ID/PASSWORD, 인증서, 스마트 카드, Kerberos등 다양한 인증 방식을 지원하기 위한 알고리즘으로 시작하여 최근에는 IETF에서 표준화를 진행중이다[7].

802.1X의 인증서버와 사용자 간의 상호 인증 방법은 네트워크에서 인증 받지 못한 AP나 “rogue"의 접속으로부터 사용자를 보호한다.

2.4 WPA와 WPA2

WPA2라 불리는 802.11i 보안 표준은 차세대 무선 보안 구조인 RSN을 드래프트 표준에 반영하였다.

RSN의 보안 목표는 첫째, 무선 보안 강화 기술을 이용한 보안의 취약성 해결, 둘째, 무선 인프라망과 AD-hoc망에 유연하게 적용할 수 있는 보안 프레임워크 제시, 셋째, 802.1X를 적용한 가입자 상호 인증 및 무선 망 접속제어, 넷째, 가입자의 제약 없는 글로벌 로밍 보안 지원, 다섯째, 액세스포인트를 이용한 가입자와 신규 서비스를 요청하는 가입자 수에 확장성이 있으면서 빠르고 안전한 재인증 메커니즘을 제공하는 것이다[3].

RSN의 주요 보안 요소는 802.1X 인증 메커니즘과 802.11i 데이터 프라이버시 메커니즘(WEP, TKIP, AES)이다. WPA는 RSN의 주요 보안 요소를 모두 제공하는 보안 서비스로서 향후 802.11i와의 호환도 가능하며, RSN으로 발전되는 보안 구조의 과도기적 단계라고 할 수 있다.

III. 실험 환경 및 결과

3.1 실험 방법

유무선이 혼재된 네트워크 상에서 유무선으로 연결된 각 Client는 무선으로 연결되어 있는 Server를 통해 데이터를 전송 받는다. 데이터는 128비트 키로 암호화하여 전송한다. 이 때, Client가 데이터를 전송받을 때까지의 시간을 측정하여, WPA의 효율성을 분석한다. 첫 번째로 10MB 이하의 데이터를 전송했을 경우와 두 번째로 50MB 이상의 데이터를 전송했을 때의 시간을 측정하였다.

실험을 위해 그림 4와 같이 하나의 AP와 유선을 통해 연결된 하나의 Client와 무선을 통해 연결된 Server와 Client로 유무선 네트워크를 구성하였다.

그림 4. 네트워크 환경

3.2 실험 결과

그림 5에서, 10MB 이하의 데이터를 전송했을 때, WPA가 설정되지 않았을 경우 약 900~1000ms의 시간이 소요되었으며, 그림 6에서 WPA를 설정한 후의 실험 결과는 약 1000~1200ms의 시간이 소요되었다. 그림 7에서, 50MB 이상의 데이터를 전송했을 때, 약 4800~6000ms가 소요되었으며, 그림 8에서 약 5800~6800ms가 소요되었다.

실험 결과, WPA의 사용 시 약 1초의 전송 지연이 발생했음을 알 수 있었다. 또한 메신저와 같은 텍스트 전송 시 전송 지연은 거의 없음을 알 수 있었다.

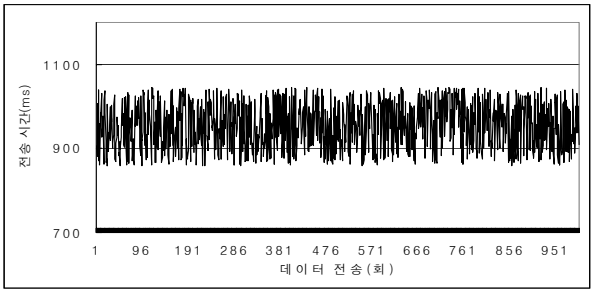

그림 5. 10MB 이하 전송

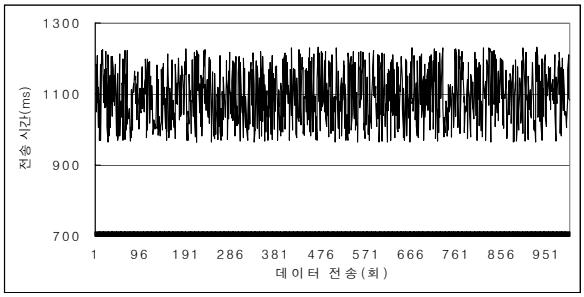

그림 6. 10MB 이하 전송(WPA)

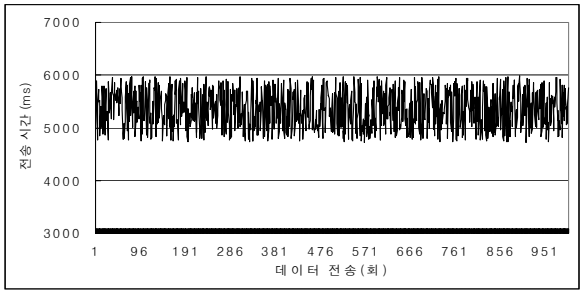

그림 7. 50MB 이상 전송

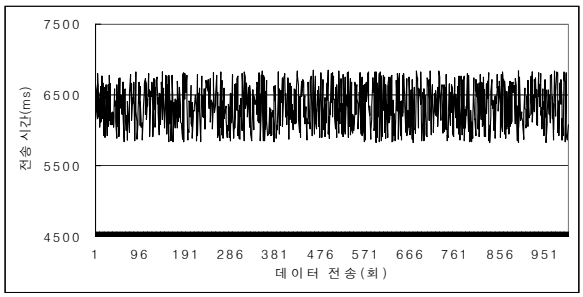

그림 8. 50MB 이상 전송(WPA)

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 WPA 보안 서비스를 이용한 전송 시간의 비교를 통해 WPA의 효율성에 대해 분석하였다. 효율성이 떨어질 것이라는 예상과는 달리 데이터 전송 시, WPA의 전송 지연은 1~2초 내외로서 인식하지 못할 만큼 작다는 걸 알 수 있었다.

향후 RSN 보안 시스템 설계를 하기 위해 WPA의 두 가지 중요 기능인 TKIP 암호화 알고리즘과 802.1X 인증 방식에 병행하여 AES 암호화 알고리즘에 대한 연구도 함께 진행 되어야 할 것이다.

참고문헌

[1] 성장렬 외, “인터넷 기반 서비스 보안요구분석” 멀티미디어학회 1998

[2] Ferguson Schenier, "PRACTICAL CRYPTOGRAPHY" 사이텍미디어 2004.4

[3] 김신효 외, “무선 LAN 정보보호 기술 표준화 동향” 정보보호학회지 2002.8

[4] 정병호 외, “공중 무선랜 망에서 인증 및 키관리 기술 동향” 전자통신동향분석 2002.8

[5] 박영호 외, “무선 LAN에서의 정보보호기술” 정보보호학회지 2002.2

[6] www.wi-fi.org

[7] 송창렬 외, “무선랜 보안 구조” 정보과학회지 2002.4