논문 15-40-03-10 The Journal of Korean Institute of Communications and Information Sciences '15-03 Vol.40 No.03
http://dx.doi.org/10.7840/kics.2015.40.3.497

PS-Net : 개인별 보안 Wi-Fi 네트워크

이 남 세◆, 이 주 호*, 정 충 교°

PS-Net : Personalized Secure Wi-Fi Networks

Nam-seh Lee◆, Ju-ho Lee*, Choong-Kyo Jeong°

요 약

기존의 보안 Wi-Fi 네트워크는 사용자가 AP(Access Point)의 암호에 맞춰야 하므로 사용이 불편하며, 사용자들이 암호를 공유하므로 시간이 갈수록 보안성이 낮아지는 문제점을 갖고 있다. 이를 해결하기 위해 사용자마다 별도의 가상 Wi-Fi 네트워크를 할당하는 방안을 제안한다. 이 방법에서는 각 사용자가 자신만의 Wi-Fi 네트워크를 가지므로 사용자 중심의 네트워크 설정이 가능하다. 사용자는 자신의 기기에 나름대로의 SSID(Service Set IDentifier)와 암호를 미리 설정해 두며 AP는 자신의 공개키를 적절한 방법으로 공개한다. AP는 또한 사용자들이 언제나 접속할 수 있는 공개채널을 유지한다. 사용자 요청이 있을 때 사용자 기기는 연결 요청 메시지를 보내는데 이 메시지에는 AP의 공개키로 암호화된 사용자 기기의 SSID와 암호가 실려 있다. 연결 요청 메시지를 받은 AP는 해당 SSID 및 암호가 설정된 새로운 가상의 AP를 생성하는데 이 가상 AP는 해당 사용자만 사용할 수 있는 전용 AP라고 할 수 있다. 이렇게 만들어지는 가상 네트워크는 비밀번호를 여러 사용자가 공유하지 않으므로 보안성이 높다. 또 이 가상 네트워크는 네트워크가 사용자 기기에 맞춰 스스로를 설정하기 때문에 사용의 편의성이 높다. 새 방법이 제공하는 보안성과 편리성에도 불구하고 기존의 Wi-Fi 네트워크에 비해 별다른 전송 능력 저하는 나타나지 않음을 실험을 통해 확인하였다.

Key Words : virtual network, wi-fi, access point, QR code, public key

ABSTRACT

Existing Wi-Fi networks require users to follow network settings of the AP (Access Point), resulting in inconveniences for users, and the password of the AP is shared by all users connected to the AP, causing security information leaks as time goes by. We propose, in this work, a personalized secure Wi-Fi network, in which each user is assigned her own virtual Wi-Fi network. One virtual Wi-Fi per user makes the user-centric network configuration possible. A user sets a pair of her own SSID and password on her device a priori, and the AP publishes its public key in a suitable way. The AP also maintains an open Wi-Fi channel, to which users can connect anytime. On user's request, the user device sends a connection request message containing a pair of SSID and password encrypted with the AP's public key. Receiving the connection request message, the AP instantiates a new virtual AP secured with the pair of SSID and password, which is dedicated to that single user device. This virtual network is securer because the password is not shared among users. It is more convenient because the network adapts itself to the user device. Experiments show that these advantages are obtained with negligible degradation in the throughput performance.

※ 본 연구는 2014년도 강원대학교 학술연구조성비로 연구하였음 (관리번호-120141528)
◆ First Author : Kangwon National University Department of Computer Engineering, namseh.lee@gmail.com, 학생회원
° Corresponding Author : Kangwon National University Department of Computer Engineering, ckjeong01@gmail.com, 종신회원
* Kangwon National University Department of Computer Engineering, alwaysshiny@gmail.com, 학생회원
논문번호 : KICS2014-11-451, Received November 4, 2014; Revised January 18, 2014; Accepted March 6, 2014

Ⅰ. 서 론

Wi-Fi에 적용할 수 있는 보안 기술과 그 침해 위협에 관해서는 오랫동안 많은 연구가 있어 왔다[1-4]. 초기에 사용되던 WEP(Wired Equivalent Privacy) 기술에 보안 취약성이 발견되어 WPA(Wi-Fi Protected Access)가 개발되었고 다시 WPA2로 발전되었다[5,6]. 기술적으로는 암호가 유출되지 않는 한 상당한 수준까지 보안성을 보장하는 단계에 와 있지만 문제는 기술 외적인 부분에서 종종 발생한다. 적지 않은 사용자가 보안설정을 하지 않거나 최초의 기본 설정을 그대로 사용한다. 그런 경우에는 신뢰할 수 없는 사용자가 AP에 접속할 수 있으므로 그로부터 여러 가지 보안 위협이 생겨난다.

대중을 대상으로 하는 공공서비스가 아닌 사설 Wi-Fi의 경우, 통상 조직 내의 폐쇄된 그룹의 이용자에게만 서비스를 제공하며 이 이용자들은 SSID와 암호를 공유한다. 하지만, 경우에 따라 소수의 외부 방문자에게도 비밀번호를 알려주어 Wi-Fi를 이용할 수 있게 하는 수가 있다. 그러면 시간이 지남에 따라 암호를 알고 있는 사람들이 많아지고 그 사람들에 의해 제 삼자에게로 암호가 추가로 유출될 위험성도 커지게 된다. 이는 곧 암호의 생명이라고 할 수 있는 비밀성이 떨어진다는 것이고 결국 네트워크 보안성이 훼손된다는 것을 의미한다.

이 연구에서는 기존 Wi-Fi에 비해 보안성과 사용자 편의성이 획기적으로 높은 사용자 중심의 Wi-Fi 네트워크 연결 방식을 제안한다. 사용자 중심 네트워크라는 것은 사용자가 네트워크에 맞춰 접속하는 것이 아니고 네크워크가 사용자의 속성에 맞춰 스스로 설정하고 사용자가 별다른 적응 과정 없이 바로 네트워크를 사용할 수 있다는 의미이다. 이렇게 하기 위해 우리는 사용자 수만큼의 가상 AP를 생성하고 각 사용자마다 전용 가상 AP를 할당하는 방법을 사용한다.

이렇게 사용자마다 전용의 가상 AP를 할당하면 각 가상 AP는 오직 한 사용자 기기만을 상대하면 되므로 스스로를 사용자 기기의 속성에 맞출 수 있게 된다. 또 이렇게 하는 경우 여러 사용자가 공유하는 암호가 필요 없으므로 암호를 공유함에 필연적으로 수반하는 암호의 비밀성 저하가 원천적으로 발생하지 않게 되고 네트워크의 보안성이 높아지게 된다.

프로토타입 구현과 이를 이용한 성능 평가에서 제안하는 방법이 편의성과 보안성의 획기적 향상에도 불구하고 전송 성능은 기존 Wi-Fi 네트워크 연결의 성능과 차이가 크지 않다는 것을 확인하였다.

이 논문의 2장에서는 관련 연구를 설명하고, 3장에서는 제안하는 PS-Net에 대한 설명과 이를 구현하는 세부 방법을 설명한다. 4장에서는 프로토타입 시스템의 구현 및 구성에 대해 서술하고, 5장에서는 PS-Net을 사용할 경우 VLAN(Virtual LAN)이 어떻게 확장될 수 있는지 설명한다. 6장에서는 PS-Net의 성능을 기존의 Wi-Fi 네트워크와 비교, 평가하고 7장에서 결론을 맺는다.

Ⅱ. 관련 연구

가상화를 통해 Wi-Fi 네트워크 서비스를 제공하는 방법에 관한 연구는 이미 여러 사례를 찾을 수 있다. Wi-Fi 네트워크를 가상화하는 데는 드라이버를 이용하여 가상화하는 방법과 가상머신을 이용하여 가상화하는 방법, 그리고 소프트웨어를 이용하여 가상화하는 방법이 있다.

Microsoft에서 발표한 MultiNet은 스위칭 알고리즘을 포함한 드라이버를 통해 하나의 물리적 인터페이스를 다수의 가상 인터페이스로 추상화화 하고, 가상 인터페이스들을 연속적으로 스위칭 하여 각 가상 인터페이스가 원활하게 네트워크에 접속되게 하는 방법을 사용한다[7].

가상 머신을 이용하여 각 인터페이스를 가상화하는 방법은 "Virtual WiFi"[8]에서 제안됐는데, 여기에서는 호스트 운영체제에 여러 개의 게스트 운영체제를 올리고, 각 게스트 운영체제에 가상 인터페이스의 프로필과 드라이버를 설정하여 다수의 무선 네트워크를 제공한다.

Microsoft의 MultiNet과 동명인 MultiNet[9]은 사용자 영역 데몬 소프트웨어를 통해 가상화하는 방법이다. 관리자는 사전에 Wi-Fi 네트워크를 이용하려는 기기의 SSID와 암호를 AP에 저장하며, 또 이 정보를 QR 코드 형태로 만들어 기기에 부착한다. 이렇게 사전에 기기를 등록한 사용자가 Wi-Fi 네트워크를 사용하고자 하는 경우 관리자는 관리자 기기를 이용해 사용자 기기의 QR 코드를 스캔하여 사용자 기기의 SSID와 암호를 얻고 이를 관리자 기기와 AP간에 상시 설정되어 있는 안전 채널을 통해 AP로 보낸다. 정보를 받은 AP는 데몬 소프트웨어를 구동하여 가상의 인터페이스를 생성하고 가상의 Wi-Fi 네트워크 서비스를 제공한다.

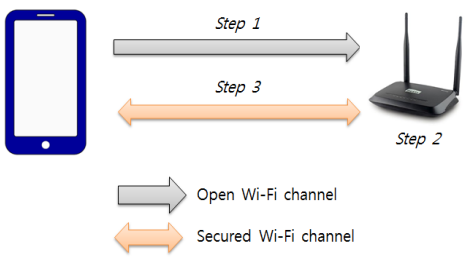
이상과 같은 여러 가지 가상화 기술들에 대한 비교 연구도 찾을 수 있다[10]. 이 연구는 각 가상화 기술들의 특징과 동작 과정을 설명하고 지원하는 기능을 비

교하였다. 가상화를 통한 AP를 제공하는 방법 외에, 2개 이상의 NIC(Network Interface Card)를 이용한 멀티 인터페이스 AP를 사용하는 방법도 있다[11]. 이 연구는 네트워크의 동적 부하 분배를 위한 연구로 목적은 다소 다르지만 두 개의 NIC를 설치하고, 운영체제를 통해 두 개의 NIC를 컨트롤 하여 다수의 Wi-Fi 네트워크를 제공하는 방법을 제안했다.

이 연구에서 우리는 MuiltiNet[9]에서 제안한 가상 네트워크 아이디어에 착안하여 사용자 편의성을 더욱 높이는 방안을 제안한다. MultiNet에서 제안한 방법과의 가장 큰 차이는 네트워크 관리자의 도움 없이 각 사용자마다의 가상 AP 설정이 자동으로 이루어진다는 점, 그리고 사전 등록이 필요 없다는 점이다. 우리는 이런 자동적인 연결이 이루어지도록 하는 구체적인 방법들을 제시한다.

Ⅲ. PS-Net

네트워크 관리자의 도움 없이 각 사용자마다의 가상 AP 설정이 자동으로 이루어지도록 하기 위해 물리적인 AP는 초기에 암호화되지 않은 공개 채널을 제공한다. 이 공개 채널은 MutiNet의 단점인 관리자 기기를 통해서만 네트워크를 구축할 수 있는 불편함을 해소하고, 사용자가 독립적으로 그리고 별다른 조작 없이 네트워크 연결을 수립할 수 있도록 해 준다. MultiNet에서 Wi-Fi 네트워크를 사용하려는 기기는 각각 SSID와 암호를 관리자가 QR코드의 형태로 사전에 등록을 해야 했다면, 제안하는 PS-Net에서는 가상 AP가 사용자 기기에 미리 설정되어 있는 SSID와 암호에 스스로를 맞춘다. 사용자 기기는 PS-Net을 지원하는 모든 Wi-Fi를 사용할 때 전혀 자신의 SSID와 암호를 변경할 필요가 없다. 네크워크가 기기에 맞추기 때문이다.



Step 1	Device information(SSID, password) is transmitted to the AP via the open channel
Step 2	A virtual AP is instantiated
Step 3	The vitual AP creates a secure channel SSID and password are set to the values protected by the device

그림 1. PS-Net 구성 절차
Fig. 1. PS-Net configuration procedure

그림 1은 PS-Net에서의 구성 절차를 보여준다. 사용자는 간단한 조작(원터치)로 Wi-Fi 연결 요청 메세지를 AP에 전달한다. 이 연결 요청 메세지에는 사용자 기기의 SSID와 암호가 포함되어 있다. AP에 정보가 전달되면, AP는 새로운 가상의 AP를 생성하고 사용자 기기의 SSID와 암호를 이용하여 AP의 보안 설정을 한다. 자신만을 위한 가상 AP가 생성되면 사용자 기기가 해당 AP에 접속하여 보안 Wi-Fi 네트워크를 이용하게 된다.

3.1 공개 채널

사용자 기기는 자신의 SSID와 비밀번호를 AP에 전송하기 위해 공개 채널을 이용한다. 공개 채널을 통해 비밀번호를 전송해야 하기 때문에 메세지를 암호화를 해야 하는데 이를 위해 RSA 암호화 알고리즘을 적용하며 AP의 공개키를 사용한다. 여기서 기기가 AP의 공개키를 얻는 방법으로는 1) AP와 가까운 공간에서 물리적 수단을 통해 알아내는 방법과 2) 보안 웹에 게시된 공개키를 읽어 오는 방법, 3) 공개 채널을 통해 알아내는 방법이 있다.

3.2 AP와 가까운 공간에서 물리적 수단을 통해 알아내는 방법

3.2.1 QR코드를 이용하는 방법

AP 관리자는 AP의 공개키를 QR 코드에 넣어 AP 근처에 게시한다. 사용자는 자신의 기기로 이 QR 코드를 스캔하여 AP의 공개키를 얻는다. 사용자 기기는 자신의 SSID와 암호를 이 공개키로 암호화하여 공개 채널을 통해 전송한다.

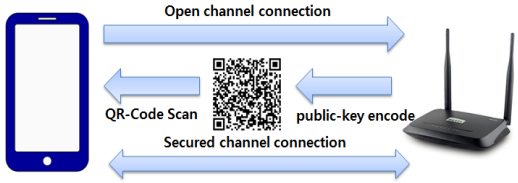


그림 2. QR 코드를 이용한 PS-Net 구성
Fig. 2. PS-Net configuration using QR codes

3.2.2 NFC 태그를 이용한 방법

NFC 태그를 이용하는 방법은 QR 코드를 이용한 방법과 유사한데, QR 코드를 이용한 방법에서는 AP

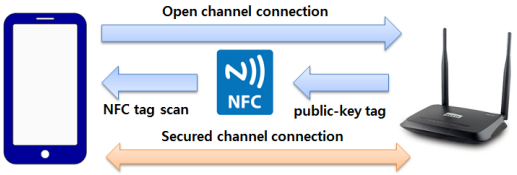


그림 3. NFC 태그를 이용한 PS-Net 구성
Fig. 3. PS-Net configuration using NFC tag

의 공개키를 QR 코드로 만들어서 공개했다면, NFC 태그를 이용한 방법은 AP의 공개키를 NFC 태그에 입력하여 공개하는 것이다. 이 방법으로 Wi-Fi를 사용하려는 기기는 이 NFC 태그를 인식하여 공개키를 얻게 되고, 이 공개키를 이용하여 자신의 SSID와 암호를 암호화하여 AP로 전송한다.

3.3 보안 웹에 게시된 공개키를 읽어 오는 방법

조직 내의 여러 AP들이 동일한 공개키를 사용할 때 적용할 수 있는 방법이고, AP가 한 대만 있을 때도 적용이 가능하다. 조직에서 운영하는 보안된 웹 페이지에 공개키를 공개하고 사용자는 이 보안 웹페이지에 접속하여 공개키를 읽어 온다. 사용자 기기는 읽어 온 공개키를 이용해 자신의 SSID와 암호를 암호화하여 AP로 보낸다. AP는 이 공개키와 쌍을 이루는 조직의 private-key를 이용해 암호를 풀어야 하는데 조직 내에 AP가 다수 있을 때 모든 AP가 조직의 private-key를 가지고 있는 것은 위험하므로 별도의 보안서버를 두어 암호 푸는 작업을 이 보안서버에 위임하는 방법을 택할 할 수 있다.

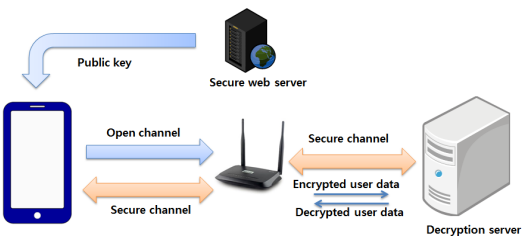


그림 4. Secure web을 이용한 공개키 배포
Fig. 4. Public-key distribution using a secure web

3.4 공개 채널을 통해 알아내는 방법

조직 내의 여러 AP들이 각각 고유의 공개키를 사용할 때 적용할 수 있는 방법이고, AP가 한 대만 있을 때도 적용이 가능하다. AP가 자신의 공개키를 공개 채널을 통해 사용자 기기로 전송한다. 주기적으로 방송하거나 사용자 기기의 요청이 있을 때 전송할 수 있다. 그러나 이렇게 하는 경우 악의적인 제 3자가 AP

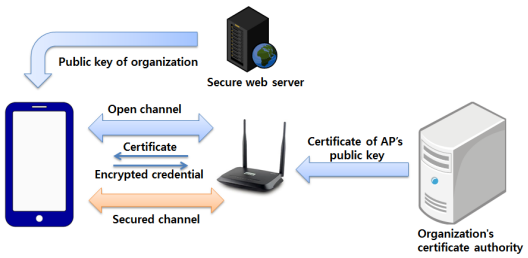


그림 5. 인증서를 이용한 공개키 배포
Fig. 5. Public-key distribution using the public key certificate

를 사칭하여 가짜 공개키를 전송함으로써 사용자 기기의 정보를 가로챌 위험이 있다. 그래서 AP가 자신의 공개키를 전송할 때는 인증서 형태로 포장해 전송해야 한다. 이 인증서에는 AP의 공개키가 적혀 있으며 AP를 관리하는 조직의 private-key를 이용한 전자서명이 들어 있다. 사용자 기기가 이 인증서의 전자서명을 확인하려면 AP를 관리하는 조직의 공개키가 필요하다. AP를 관리하는 조직의 공개 키는 조직에서 운영하는 보안된 웹 페이지에 공개된다.

3.5 AP 가상화를 통한 네트워크 연결

위에서 설명한 방법들을 통해 AP는 네트워크를 사용하려는 기기의 SSID와 암호를 얻었다. 이제 AP는 해당 사용자 기기를 전담해 서비스할 가상의 AP를 하나 생성한다. 가상 서버를 생성하는 기술은 이미 널리 알려져 있으며 우리는 리눅스 기반 시스템에서 hostapd[12]를 이용하였다. 새로이 생성된 가상 AP는 전달 받은 SSID와 암호에 맞춰 자신을 설정한다. 이 과정을 통해 네트워크가 생성되면 기기는 이 SSID를 확인하고 암호를 이용하여 보안 네트워크와의 연결을 시도한다. 연결이 수립되면 이 가상화된 AP 네트워크를 이용하는 기기는 단 하나가 되며 다른 사용자들은 해당 패스워드를 알지 못하는 한 이 가상 AP에 접속할 수 없다.

Ⅳ. 프로토타입 시스템 구현

제안하는 기술의 타당성과 편의성을 검증하기 위해 프로토타입 시스템을 구현하였다. 프로토타입 시스템에서는 이 논문에서 설명한 하는 방법 중 QR 코드를 이용한 가장 간단한 방법을 구현하였다. 전체 시스템의 구성은 그림 6 과 같다. 사용자 기기로는 안드로이드 스마트폰을 이용하였으며 기기의 기본 SSID와 암호를 임의로 설정하는 기능과 원 터치 요청으로 가상

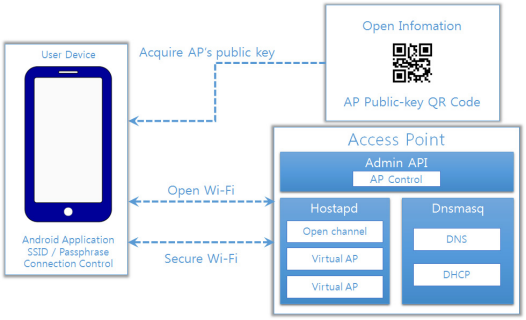


그림 6. 전체 시스템 구성
Fig. 6. System configuration

Wi-Fi에 접속하는 기능을 가진 앱을 구현하였다. 네트워크 기능과 무선 관리 기능을 담당하는 AP는 라즈베리파이[13,14] 싱글보드 컴퓨터에 EFM 네트웍스의 ipTIME N150UA 무선 랜 카드[15]를 장착한 하드웨어와 라즈비안 리눅스[16]를 기반으로 구성하였다. AP 서비스 가상화를 위해서는 hostapd와 dnsmasq[17]를 이용하였다. 그리고 파이썬으로 작성한 AdminAPI를 통해 제어가 가능하도록 시스템을 구성하였다.

4.1 안드로이드 앱

사용자는 사전에 안드로이드 앱의 “Setting” 버튼을 통해 기기의 기본 SSID와 암호를 설정하여 저장한다. SSID와 암호를 설정하는 이 조작은 단 한 번만 하면 된다. 물론 사용자가 기기의 SSID와 암호를 변경하고 싶으면 언제든지 바꿀 수 있다. 이후 네크워크 접속이 필요할 때 사용자가 “QR Scan” 버튼을 누르면 QR 코드 스캔 앱으로 이어진다. 사용자는 AP 근처에 부착되어 있는 AP의 공개키 QR 코드를 스캔하고, 스캔이 정상적으로 완료되면 앱은 AP의 공개키를 확보하게 된다. 공개키를 확보하면, 앱은 공개 채널에 자동으로 접속하고, 위에서 설명한 방법에 따라 SSID와 암호를 AP의 공개키를 이용해 암호화 후 AP에 전달한다. AP는 전달 받은 정보를 이용하여 가상의 AP를 생성하고, 앱은 이를 확인하고 공개 채널과의 연결을 해지한 후 새로 생성된 가상의 AP에 접속한다.

4.2 Access Point(AP)

4.2.1 hostapd와 dnsmasq

hostapd는 리눅스에서 master mode가 가능한 무선 랜카드를 이용하여 AP로서의 역할 수행이 가능하도록 만들어 주는 데몬이다. hostapd는 무선 랜의 인터페이스를 master mode로 변경하고, SSID를 부여하여 사용자가 Wi-Fi 네트워크에 접속이 가능하도록 만들어 준다. 프로토타입 AP에서는 hostapd의 “Multiple BSSID support” 기능을 활용하여 다수의 가상 AP를 생성하도록 한다. “Multiple BSSID support” 기능은 설정파일에서 BSS와 BSSID, SSID 그리고 보안 설정을 입력하면 입력한 값에 따라 SSID 및 보안설정을 갖는 가상의 인터페이스를 생성한다. dnsmasq는 DNS, DHCP 기능을 제공하는 프로그램으로서 hostapd에서 가상으로 생성되는 인터페이스들에게 IP 주소를 부여하고 DNS 역할을 함과 동시에, 각 인터페이스들에 대해 DHCP 기능이 지원되도록 한다.

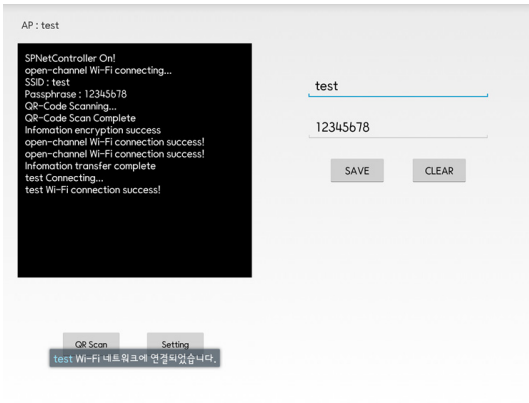


그림 7. 안드로이드 앱 동작 및 설정 화면
Fig. 7. Android App operation and setting screen

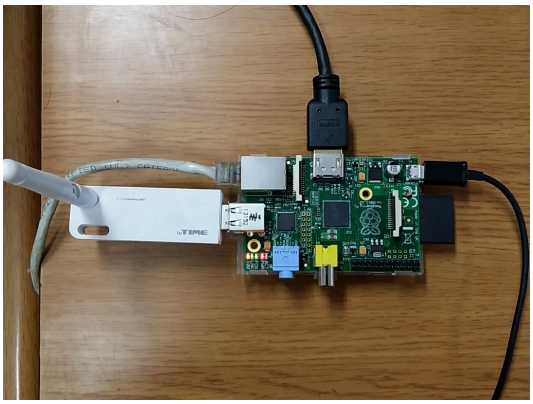


그림 8. 라즈베리파이를 이용하여 구현한 AP
Fig. 8. Prototype AP based on raspberry-pi

4.2.2 AdminAPI

위에서 설명한 hostapd와 dnsmasq 및 기타 리눅스 명령들은 일련의 스크립트로 작성하여 실행 할 수 있으나, 우리는 AP 관리의 편의성을 고려하여 RESTful 서비스[18] 형태의 AdminAPI를 구현하였다. AP 관리를 위한 각 서비스 요청은 URL을 지정하는 방식으로

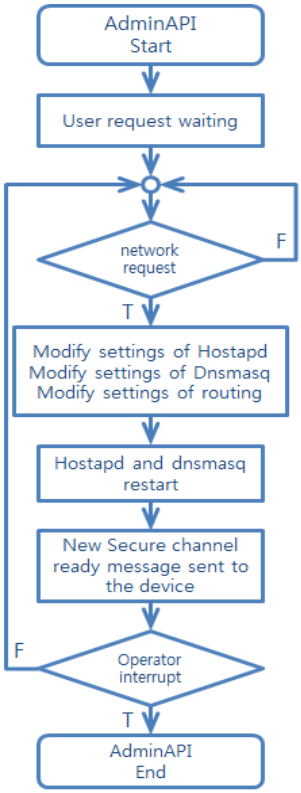


그림 9. AdminAPI 순서도
Fig. 9. AdminAPI flowchart

이루어진다. 사용자 기기의 앱 역시 http 프로토콜을 이용하여 암호화된 데이터를 해당 서비스 URL로 전달한다. AdminAPI 서비스는 hostapd에 대한 SSID와 암호 설정이 끝나면, 가상으로 생성된 인터페이스의 IP 할당과 dnsmasq 설정을 통해 DHCP가 동작 할 수 있도록 설정한다. 다음으로는 리눅스의 iptables 명령을 이용하여 유선 랜과 각 무선 랜 인터페이스 간의 라우팅 경로를 설정하여 가상의 AP가 정상적으로 네트워크를 이용할 수 있도록 한다.

V. 성능 평가

PS-Net은 한 대의 물리적인 기계에 여러 개의 가상 AP를 생성하고 이 가상 AP들을 병렬로 작동시키므로 기존 AP에 비해, 소프트웨어 처리 부하가 약간 많아지고, 무선 채널의 이용 효율이 조금 낮아지게 된다. 특히, 하나의 무선 주파수 채널을 공유하는 가상 AP를 여러 개 만들면 각 가상 AP가 각각 일정한 간격(100 msec)마다 비이컨(beacon) 신호를 방송해야 한다. 만약 단말기 쪽에서 probe request를 보내면 이에 대해 모든 가상 AP가 probe response를 보낸다. 따라서 하나의 채널에 하나의 AP가 하나의 SSID만을 사용하는 경우에 비해 무선 채널의 오버헤드가 늘어나게 마련이다. 이 두 가지 요인에 의한 성능 저하가 실제 이용 환경에서 얼마나 되는지 알아보기 위해 프로토타입 시스템을 이용하여 데이터 전송률을 측정하였다. 물리적인 AP 하나만을 사용하도록 프로토타입 시스템을 설정하여 기존의 Wi-Fi와 같은 환경을 만들고 단말기들의 전송률을 측정한 후, 이 연구에서 제안한 방법으로 프로토타입 시스템을 설정하여 단말기들의 Wi-Fi 전송률을 측정하여 비교하였다.

트래픽 발생과 전송률 측정을 위해서는 네트워크 성능 측정 및 파라미터 튜닝에 널이 쓰이는 Iperf[19]를 사용했다. 트래픽을 보내고 받는 서버와 클라이언트는 처리 능력과 송수신 능력이 충분해야 하고, 측정 대상인 무선 구간이 데이터 송수신의 병목이 되도록 해야 하므로, Iperf 서버와 클라이언트를 모두 iMac 컴퓨터에서 실행하였다. 서버는 AP의 유선 LAN 포트에 컴퓨터를 한 대 연결하여 실행했고 클라이언트들은 Wi-Fi를 통해 무선으로 연결된 컴퓨터들에서 실행하되 한 컴퓨터에는 하나의 클라이언트만 실행시켰다. 클라이언트들은 모두 하나의 서버와 트래픽을 주고받으면서 각 연결의 전송률을 측정한다.

Wi-Fi에 접속한 컴퓨터의 수를 증가시키면서 60초 동안 다운로드와 업로드 전송률을 측정하되 각 3회씩 반복하여 평균값을 얻는 실험을 진행하였다. 그림 10은 Wi-Fi에 접속한 클라이언트 수에 따른 전송률 변화를 나타낸 그래프이다. AP에 연결된 클라이언트가 많아짐에 따라 각 클라이언트의 전송률이 떨어지는데 이 전송률의 합은 거의 일정한 값을 유지하므로 일반적으로 보아 클라이언트 수가 크지 않은 범위에서는 다중접속에 의한 성능 저하가 뚜렷하게 나타나지 않음을 볼 수 있다. 또, 고전적인 AP와 제안한 방법을 따르는 AP을 비교하면 클라이언트 수가 증가함에 따른 전송률 감소 추세에 별다른 차이가 없음을 볼 수 있다. 이는 클라이언트 수가 크지 않은 범위에서는 여러 개의 가상 AP를 운영함에 따르는 오버헤드가 실용적으로 문제가 되지 않을 정도로 작다는 것을 의미한다. 만약 가상 AP 수가 매우 커지면 이 오버헤드도 무시하지 못할 만큼 커질 가능성이 있다. 그러나 이 실험에서는 클라이언트를 다섯 대 이상 연결하는 경우 전송률이 지나치게 낮아져 실용적으로 의미가 없는 수준으로 떨어졌으므로 그 이상의 클라이언트 수에 대해서는 측정을 하지 않았다. 다섯 대 이상의 클라이언트에 대해 전송률이 지나치게 낮게 나오는 것은 프

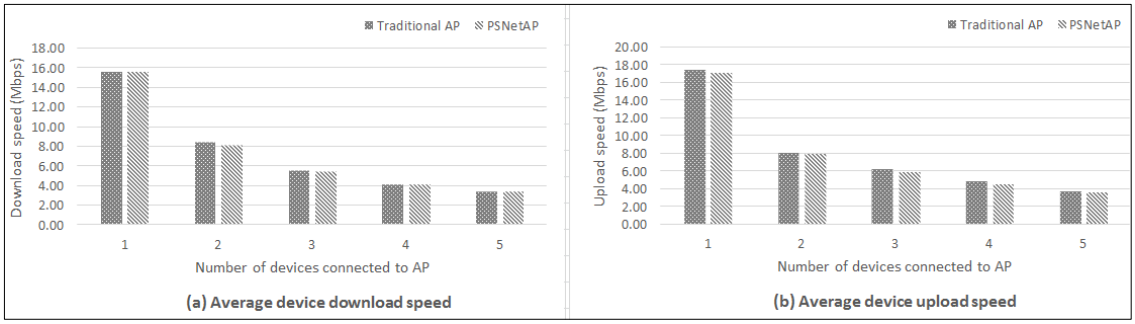


그림 10. 전통적인 AP와 PS-Net AP의 다운로드 및 업로드 성능 비교
Fig. 10. Download and upload throughput comparison between traditional AP and PS-Net AP

로토타입 AP를 구현하는 데 사용한 싱글보드 컴퓨터 하드웨어와 랜 카드의 낮은 성능과 학교 실험실 주변의 고밀도 무선 환경 등의 탓이라고 생각된다. 우리는 또, iMac과 Iperf 대신 일반적으로 사용하는 여러 가지 안드로이드 스마트폰들에 안드로이드 “벤치비” 속도측정 앱[20]을 설치하여 동일한 실험을 수행했다. 이 실험 결과는 그림 10 과 크게 다르지 않아 이 논문에 제시하지 않는다. 다만, 스마트폰을 이용해 시험한 경우 스마트폰 기종에 따라 스마트폰간 전송률 편차가 꽤 많이 있음을 볼 수 있었다. 그러나 각 디바이스의 평균 전송률에 있어서는 그림 10 과 유사한 결과를 볼 수 있었다.

Ⅵ. PS-Net의 기타 응용 - VLAN

VLAN은 기존 유선 네트워크에서 여러 개의 스위치에 분산되어 있는 포트들을 물리적 위치와 무관하게 링크 계층에서 여러 그룹으로 묶어 여러 개의 가상의 랜을 구성하는 기술이다. 해당 기술은 각 논리적 그룹의 내부 자원의 보안을 높일 수 있고, 그룹 멤버의 이동이 필요한 경우 물리적 장비 이동 대신 간단한 네트워크 설정만으로 해결할 수 있다. 또한 VLAN 네트워크 그룹에서 브로드캐스트 패킷이 다른 VLAN 그룹에게 전송되지 않음으로써 트래픽의 낭비를 줄일 수 있는 이점이 있다.

하지만 이 기술은 기존의 Wi-Fi 네트워크에서는 적용하기 어렵다. AP의 Wi-Fi 네트워크에 연결된 기기들은 AP의 관리를 받는 하나의 그룹으로 되기 때문이다. 하지만 제안하는 PS-Net을 이용하는 경우 각 사용자 연결이 독립적인 서브넷을 이루므로 각 사용자 기기 하나 하나를 적절한 VLAN에 편입시킬 수 있게 된다.

기기에 사용자의 그룹 정보를 입력하고, 제안하는 PS-Net의 네트워크에 연결을 요청하면 AP는 사용자가 속한 그룹을 구분할 수 있게 되며 그룹 정보를 바탕으로 해당 그룹의 가상화된 네트워크들을 VLAN의 형태로 묶어준다. 물론 하나의 AP에서 생성한 다른 가상화된 네트워크들만으로 VLAN을 구성할 수도 있지만 다른 AP에서 생성한 가상화된 네트워크들도 하나의 VLAN 그룹에 포함하여 구성할 수도 있다. 따라서 제안하는 PS-Net을 이용한다면 유선 네트워크에서만 이용이 가능했던 VLAN 기술을 Wi-Fi 네트워크 환경까지 확장해서 이용할 수 있다.

Ⅶ. 결 론

이 연구에서는 AP의 설정에 따라 사용자가 Wi-Fi 네트워크를 이용하는 것이 아니라, AP가 사용자 설정에 맞춰 Wi-Fi 네트워크를 제공하는 방안과 그 구체적 구현 방안들을 제시하고 실험을 통해 현실적 실현 가능성을 확인하였다. 이 방법을 사용하면 사용자가 네트워크 관리자로부터 AP의 보안 암호를 얻어 사용자 기기에 설정하는 번거로움 없이, 사용자 기기에서의 간단한 조작만을 통해 암호가 설정된 보안 Wi-Fi 네트워크를 이용할 수 있다. 또한, 각 사용자는 자기만의 암호를 사용하므로, AP의 보안 암호를 여러 사용자들이 공유함으로써 시간이 지남에 따라 암호의 비밀성이 점차 훼손되어 발생하는 보안성 저하 문제가 원천적으로 발생하지 않게 된다. 이 연구에서는 이 기술을 실현하는 세 가지 구현 방안을 제시했는데 네트워크 규모나 네트워크를 사용하는 조직의 성격에 따라 적당한 방법을 선택하여 적용하면 될 것이다. 여러 개의 가상 네트워크를 생성하여 한 주파수 채널에서 두 개 이상의 Wi-Fi 네트워크를 운영하는 탓에 약간의 오버헤드가 발생하기는 하지만 실질적으로는 이용에 문제가 되지 않는 정도임을 실험적으로 확인하였다.

References

[1] T. Rowan, "Negotiating wifi security," *Network Security*, vol. 2010, no. 2, pp. 8-12, Feb. 2010.

[2] H. Jahankhani, D. L. Watson, and G. Me, *Wi-fi security*, Handbook of Electronic Security and Digital Forensics, World Scientific Publishing Company, pp. 83-92, Nov. 2009.

[3] D. O. Shin, J. Kang, D. H. Nyang, S. Lee, and K. H. Lee, "A method of authenticating WLAN APs for smartphones," *J. KICS*, vol. 39B, No. 01, pp. 17-28, Jan. 2014.

[4] J. Park, M. Park, and S. Jung, "A whitelist-based scheme for detecting and preventing unauthorized AP access using mobile device," *J. KICS,* vol. 38B, No. 08, pp. 632-640, Sept. 2013.

[5] Wi-Fi Alliance, *Introducing Wi-Fi Protected Setup™(2007)*, Retrieved Jan. 18. 2015, from http://www.wi-fi.org/

[6] Wi-Fi Alliance, *The State of Wi-Fi® Security(2012)*, Retrieved Jan. 18. 2015. from http://www.wi-fi.org/

[7] R. Chandra and P. Bahl, "MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card," in *INFOCOM 23rd Annu. Joint Conf. IEEE Comput. and Commun. Societies.*, vol. 2, 2004.

[8] L. Xia, S. Kumar, X. Yang, P. Gopalakrishnan, Y. Liu, S. Schoenberg, and X. Guo, "Virtual WiFi: Bring virtualization from wired to wireless," *ACM SIGPLAN Notices*, vol. 46, no. 7, pp. 181-192, Jul. 2011.

[9] A. Brown, R. Mortier, and T. Rodden "MultiNet: usable and secure WiFi device association," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42. no. 4 pp. 275-276, Oct. 2012.

[10] J. Kim and Y.-B. Ko, "On the AP Virtualization of IEEE 802.11 WLANs," *Int. Conf. Green and Human Inf. Technol.*, Ho Chi Minh City, Vietnam, 2014.

[11] T. Kim, H.-Y. Seo, and J.-D. Kim, "Design and Implementation of a Multi-Interface Access Point with Inter-interface Dynamic Load Balancing," *J. KICS*, vol. 37A, no. 05, pp. 348-357, May 2012.

[12] Malinen, Jouni. hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator(2013), Retrieved Jan. 18. 2015. from http://w1.fi/hostapd/

[13] E. Upton and G. Halfacree, *Raspberry Pi user guide*, John Wiley & Sons Inc., 2013.

[14] S. Monk, *Programming the Raspberry Pi: Getting Started with Python*, Mcgraw-hill, 2013.

[15] EFM Networks, ipTime N150UA(2014), Retrieved Jan. 18. 2015, from http://www.iptime.co.kr/~iptime/prd.php?pf=9&page=&pt=42&pd=1

[16] A. Kurniawan, *Raspberry Pi System Programming for Beginner*, PE Press, 2014.

[17] Dnsmasq, *Dnsmasq*(2014), Retrieved Jan. 18. 2015, from http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html

[18] L. Richardson and S. Ruby, *RESTful web services*, O'Reilly Media, Inc., 2008.

[19] Iperf, *Iperf*(2014), Retrieved Jan. 18. 2015, from https://iperf.fr/

[20] Benchbee, *Benchbee mobile(2014)*, Retrieved Jan. 18. 2015, from http://www.benchbee.co.kr/09center/mobile/

이 남 세 (Nam-seh Lee)

2012년 2월 : 강원대학교 컴퓨터학부 학사

2015년 2월 : 강원대학교 컴퓨터정보통신공학과 석사

<관심분야> 유/무선 네트워크, 웹 서비스, 클라우드 컴퓨팅

이 주 호 (Ju-ho Lee)

2005년 : 강원대학교 전기전자정보통신공학부 학사
2007년 : 강원대학교 컴퓨터정보통신공학과 석사
2011년~현재 : 강원대학교 컴퓨터정보통신공학과 박사과정

<관심분야> 이동통신, 빅데이터, Cloud Computing, VoIP, Embedded Linux

정 충 교 (Choong-Kyo Jeong)

1982년 2월 : 서울대학교 전기공학과 학사
1984년 2월 : 한국과학기술원 전기전자공학과 석사
1989년 2월 : 한국과학기술원 전기전자공학과 박사
1995년 3월~현재 : 강원대학교 컴퓨터학부 교수

<관심분야> 통신프로토콜, 통신망성능분석, 이동통신, 네트워크보안