논문번호 12-37C-09-09

한국통신학회논문지 '12-09 Vol.37C No.09
http://dx.doi.org/10.7840/kics.2012.37C.9.821

SNS 기반 무선랜 정보 공유 시스템 설계 및 구현

우 연 경◆, 최 준 혁*, 박 종 태°

Design and Implementation of Wireless LAN Information Sharing Based on SNS

Yeon-Kyung Woo◆, Jun-Hyuk Choi*, Jong-Tae Park°

요 약

최근 들어, 저비용의 모바일 멀티미디어 서비스를 받기 위해 사용자의 무선랜 (WLAN) 사용에 대한 요구사항이 크게 증가하고 있다. 하지만 기존의 무선랜 시스템은 Open Authentication 방법에 의한 AP에 접속함으로써 외부공격에 취약하다. 본 논문에서는 무선랜 보안키를 안전하고 효율적으로 관리하는 SNS 기반 무선랜 접근 공유 시스템을 설계 및 구현하였다. 본 논문에서 제안한 무선랜 접근 공유 모델에서 사용자들 간의 무선랜 접근 권한을 위해 사회적 신뢰강도를 제안한다.

Key words : 무선랜, SNS 기반, 신뢰강도

ABSTRACT

Recently, in order to provide the mobile multimedia service cost-effectively, the user's demand has been greatly increasing to use wireless LAN (WLAN). But existing WLAN (Wireless LAN) is vulnerable to attack of outside, as users are connecting AP using Open Authentication. In this article, we have designed and implemented WLAN Information Sharing System using social network service (SNS) which is efficiently managing. WLAN secure key. A proposed WLAN Information Sharing System model has been proposed in which the social trust strength between people is employed for WLAN access control.

Ⅰ. 서 론

최근들어 WiFi, 3G와 4G 이동통신 서비스를 통해 다양한 멀티미디어 서비스를 사용하고자 하는 사용자가 증가하고 있다. 사용자가 무선랜 (WLAN: Wireless Local Area Network) 에 접속하기 위해서는 탐색, 인증, 결합과정 후 AP (Access Point: 접속점) 를 경유한 데이터 전송과정이 수행된다[1]. 무선랜 (IEEE 802.11 a/b/g/n [ ])은 사용인증 허가가 필요 없는 ISM 대역의 주파수를 사용하여 최소 10 Mbps에서 최대 600 Mbps 까지의 전송률 (Data Rate) 을 제공 한다[2]. 하지만 일반적인 기존 무선랜 단말은 인증절차가 없는 Open Authentication 방법을 사용하여 AP에 접속하고, 무선구간을 평문으로 전송한다. 이러한 방법은 서비스 거부 공격에 취약할 뿐만 아니라, 사용료를 지불하지 않은 사용자들도 아무런 제약 없이 AP를 거쳐 내부망이나 외부망을 사용할 수 있을 뿐만 아니라, 전송되는 프레임의 내용

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터 지원사업 (NIPA-2012-(C1090-1121-0002)), 2단계 BK21 프로젝트 및 경북대학교 학술연구비에 의하여 연구 되었음.
◆ 주저자 : 경북대학교 전자전기컴퓨터학부 정보통신망 신기술 연구실, ykwoo@ee.knu.ac.kr, 준회원
° 교신저자 : 경북대학교 전자전기컴퓨터학부 정보통신망 신기술 연구실, jtpark@ee.knu.ac.kr, 종신회원
* 경북대학교 전자전기컴퓨터학부 정보통신망 신기술 연구실, jhchoi1@ee.knu.ac.kr, 준회원
논문번호 : KICS2012-04-216, 접수일자 : 2012년 4월 24일, 최종논문접수일자 : 2012년 9월 3일

이 노출되거나 변조되는 문제가 있다[1]. 이를 개선하기 위하여 무선랜에 접속하기 위한 무선랜 보안키를 안전하고 효율적으로 관리하는 방법이 필요하다. 무선랜 보안키를 안전하고 효율적으로 관리하는 방법 중의 하나는 사용자들 간에 보안키를 안전하게 공유하는 것이다.

최근에, 무선랜 공유 서비스 업체인 Fon과 Whisher가 무선랜을 제공하고 있다. 스페인에 본사를 둔 FON은 사용자들이 무선랜을 공동으로 활용하는 사업모델을 개발하여 유럽과 미국 등에서 서비스를 제공하고 있다[5]. FON은 개인이 커뮤니티에 등록한 뒤 자신의 AP를 회원들과 공유하는 형태의 서비스로, 자신의 무선랜이 켜져 있을 때에는 전 세계 어디서나 다른 회원의 무선 네트워크를 무료로 사용할 수 있는 무선랜 공유 서비스를 제공하고 있다. 하지만 무선랜에 WRT 기반의 펌웨어가 설치되어 있는 사용자들에 한하여 자신의 AP를 공유할 수 있다는 단점이 있다. 또한 무선랜 공유 서비스 업체인 Whisher는 '친구 공유', '개인', 'Add as VIP' 의 세 가지 모드로 구성되어 있으며, 최초 무선랜을 등록하고 공유 방식을 지정해두면, 그 다음부터는 PC를 끄거나 자리를 비우더라도 다른 사람들이 접속할 수 있는 무선랜 공유 서비스를 제공한다.

하지만 이들 서비스는 데이터 도청이나 인가되지 않은 사용자가 쉽게 악의적으로 접근할 수 있는 취약성을 가지고 있어 보안이 설정되어 있지 않은 무선랜 인프라가 구축된 곳에는 인가된 사용자나 악의적인 목적을 가진 공격자이건 간에 무선랜이 설치된 주변에 있는 사용자는 누구나 자동으로 원치 않는 타인과 공유될 수 있다는 문제점이 있다. 또한 무선랜 등록 과정에서 사용자는 오류 문제와 같은 불편함을 겪고 있다. 이러한 문제점을 해결하기 위한 새로운 무선랜 공유 서비스 방법이 필요하다.

현재 안드로이드, i-OS, 등의 모바일 플랫폼 기반의 스마트 이동단말의 전 세계적으로 보급됨에 따라 SNS (Social Network Service) 를 사용하는 사용자가 폭발적으로 증가하고 있다. 대표적인 SNS인 미국의 Facebook은 현재 전 세계적으로 8억명 이상의 가입자를 확보하고 있다[3]. 지금까지 개발된 대부분 SNS는 동창, 친구 및 기타 사람 간 관계를 맺어주고 개인정보를 공유하고, 친구목록 등을 사용하여 사람들 간의 사회적 관계를 확대하는 방법을 제공한다. 예를 들어, 미국의 Facebook이나 한국의 대표적 SNS인 싸이월드 등 대부분의 기존 SNS 시스템은 사람들 간의 관계 설정 및 친구의 친구 (Friends of Friends) 를 사용한 사람들 간의 관계 확충, 친구관계의 신뢰 (Trust) 에 따른 개인정보 공유 여부 등의 기능을 제공한다. 미국 Myspace 경우에는 SNS를 통하여 친구들 간에 음악, 비디오, 게임 등을 공유하게 한다[4]. SNS는 동적인 가상 조직을 만들고 사용자들이 서로 간의 정보를 공유할 수 있도록 서비스를 제공한다. 그러나 상기 대부분의 SNS는 가입자 간 신뢰관계에 따른 개인정보의 공유기능을 제공하지만 신뢰강도에 따른 차별화된 안전한 무선랜 공유 방법을 제공하지 않는다. 여기서, 신뢰강도란, 지인 또는 친구간의 관계 정도를 나타낸다.

본 논문에서는 안전하고 효율적으로 무선랜 공유하기위한 SNS 신뢰강도 기반의 무선랜 접근 공유 시스템 설계 및 구현하였다. 이를 위해 SNS 신뢰강도 기반의 무선랜 접근 공유 모델을 제시하고, 이를 기반으로한 SNS 신뢰강도 기반 무선랜 공유 시스템 구조를 설계하고, 구현을 통해 제공 서비스 기능을 검증한다.

본 논문은 다음과 같이 구성된다. 2장에서는 SNS 신뢰강도 기반의 무선랜 접근 공유 SNS 모델 및 구조에 대해 알아보고, 3장에서는 제안한 SNS 신뢰강도 기반의 무선랜 접근 공유 시스템을 구현하였으며 끝으로 4장에서 결론을 맺는다.

Ⅱ. SNS 신뢰강도 기반의 무선랜 정보 공유 모델 및 시스템 구조

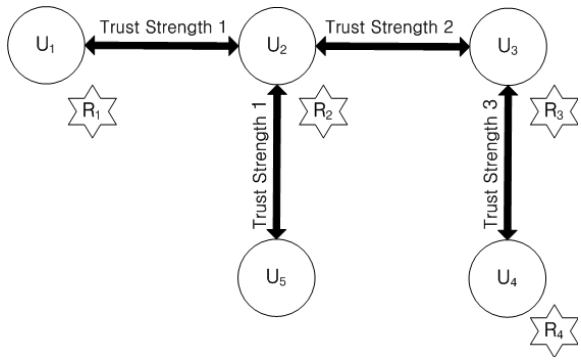


그림 1. 신뢰강도기반 무선랜 정보 공유 모델
Fig. 1. WLAN Information Sharing Model based Trust Strength

2.1. SNS 신뢰강도 기반의 무선랜 정보 공유 모델

그림 1은 다양한 신뢰강도의 친구관계로 구성된 무선랜 접근 공유 모델을 나타낸다. 그림 1에서 원은 사용자를 나타내며, 별표는 무선랜 접근정보, 즉 SSID (Service Set Identifier), BSSID (Base Station

Service Identifier), 인증키 등을 나타낸다. 사용자간의 양방향 화살표는 사용자간의 신뢰강도 (Trust Strength) 를 나타낸다. 여기서 신뢰강도는 친구 또는 지인 등의 사용자들 간에 사회적 관계를 나타낸다. 본 시스템에서의 신뢰강도는 사용자들 간의 무선랜 서비스 사용 요청/확인 메시지를 통해 생성된 관계의 강도를 나타낸다.

예를 들어, 그림 1에서 다양한 형태의 사회적 네트워크 관계 (Social Network Relationship)가 적용될 수 있다. 그림 1에서 사용자 U1, U2, U3, U4가 서로 간에 각각 다른 신뢰등급을 가지고 상호간에 무선랜 접근 비밀번호를 공유한다. 사용자 U1, U2, U3 및 U4는 무선랜 R1, R2, R3 및 R4를 각각 소유한다. 사용자 U1과 U2는 서로 간에 신뢰강도 1의 친구관계로 친구사이에서만 무선랜 접근 권한 공유가 가능하고 한 단계 건너 친구에게는 무선랜 접근 권한 공유가 가능하지 않다. 따라서 무선랜 R1과 R2를 공유하고, 사용자 U2과 U3는 서로 간에 신뢰강도 2의 친구관계로 무선랜 R2과 R3를 공유한다. 사용자 U3과 U4는 서로 간에 신뢰강도 3의 친구관계로 무선랜 R3와 R4를 공유한다. 마지막으로 사용자 U2와 U5는 신뢰강도 1의 친구관계로 사용자 U5가 사용자 U2의 무선랜 R2를 공유하며, 사용자 U5는 공유할 무선랜이 없기 때문에 U2에 제공할 것이 없다. 그림 1에서 U1과 U2는 신뢰강도 1를 가진 친구관계 (Friend Relationship)을 가진다. U1과 U3 및 U1과 U5는 상호간에 친구의 친구 (FoF: Friend of Friend)인 친구관계를 가지고, U1과 U4는 상호간에 친구의 친구의 친구 (FoFoF: Friend of FoF)인 친구관계를 가진다. 표 1은 신뢰등급에 따른 공유 권한을 보인다. 신뢰등급이란 무선랜 공유를 위해 친구 상호간에 믿을 수 있는 등급을 말한다. 신뢰강도 1은 상호 친구관계에 있는 사용자에게만 무선랜 공유 권한을 부여한다. 즉, U1 및 U2는 서로 친구관계이기 때문에 자기의 무선랜에 대한 공유 권한을 상대방에게 부여하여 상호 무선랜을 공유한다. 그러나 U3, U4 및 U5는 U1의 무선랜 접근 권한이 없다. 왜냐하면 U1가 U2와 신뢰강도 1이기 때문에 U1은 단지 U2에게만 무선랜 공유를 허용하기 때문이다. 그림 1에서 U2와 U3는 신뢰강도 2를 가진다. 표 1에서 신뢰강도 2는 친구관계인 상대방뿐만 아니라 친구의 친구 (FoF)에게도 자기가 가지고 있는 무선랜 접근을 허용한다. 그러므로 U2및 U3는 각각 자기가 가지고 있는 무선랜을 서로 간에 공유하며, 서로의 FoF인 U1, U4 및 U5에게도 무선랜 공유를 허용한다. 즉, 표 1에서 신뢰강도 2 관계는 친구의 친구 (FoF)에 대한 무선랜 공유를 허용하며 U5는 U2를 통해 U3의 무선랜에 대한 접근이 가능하고, U1은 U2를 통해 U3의 무선랜에 대한 접근을 허용한다. 마지막으로 U3과 U4는 상호간에 신뢰강도 3인 신뢰강도를 가지고 친구관계를 형성하며, 표 1에서 신뢰강도 3은 친구 (F), 친구의 친구 (FoF)뿐만 아니라 친구의 친구의 친구 (FoFoF)에게도 자기가 가진 무선랜에 접근 권한을 부여한다. 그러므로 U1은 U4의 무선랜을 접근 할 수가 있으며 U4는 U1의 무선랜을 접근할 수 없다.

표 1. 일반화된 신뢰강도별 접근 권한 공유
Table 1. Access Right of Trust Strengh

Trust Strength	Access right to resource object
Trust Strength 1	Friend
Trust Strength 2	Friend and FoF
Trust Strength 3	Friend, FoF, FoFoF
:	:
Trust Strength N	Friend, FoF, …, Fo…oF

본 논문에서는 무선랜 공유를 위한 구체적 전송 통신 프로토콜은 제시하지 않는다. 전송방법으로 P2P, Cloud Computing, HTTP등 다양한 인터넷 응용 통신 프로토콜들이 사용 가능하다.

지금까지 정의된 신뢰강도 기반의 무선랜 접근 공유를 위한 SNS 모델에서 몇 가지 성질을 정의한다.

Property 1 : 사용자 A가 친구관계를 맺을 수 있는 최대 신뢰강도가 k이면 신뢰강도 k보다 큰 신뢰강도를 가진 있는 사용자는 무선랜 접근 공유를 위한 친구관계로 고려할 필요가 없다.

Property 2 : 동일한 무선랜에 대해 상위 신뢰강도의 무선랜 공유 권한은 하위 신뢰강도가 가진 모든 무선 공유 권한을 갖는다. 표 1에서 신뢰강도 2는 신뢰강도 1이 가진 무선랜 공유 권한을 모두 갖는다. 왜냐하면 신뢰강도 2는 친구의 친구에게도 무선랜 공유 권한을 허용하기 때문이다.

2.2 SNS 신뢰강도 기반의 무선랜 정보 공유 시스템 구조

2.2.1. 무선랜 접근 공유 클라이언트 시스템 구조

그림 2는 SNS 기반의 무선랜 접근 공유 클라이언트의 구조도이다. 안드로이드 플랫폼 상에서 동작

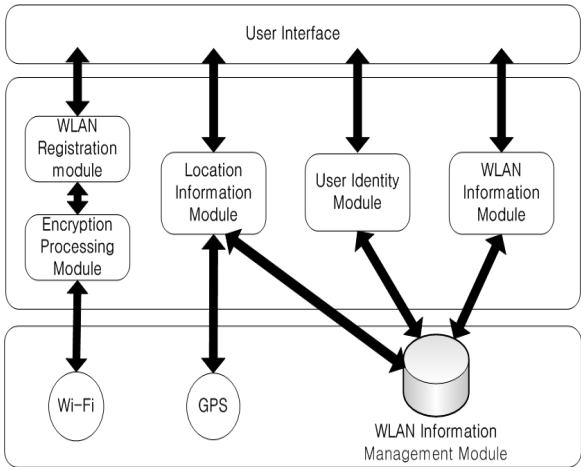


그림 2. 무선랜 정보 공유 클라이언트 시스템 구조도
Fig. 2. Architecture of WLAN Access Sharing Client

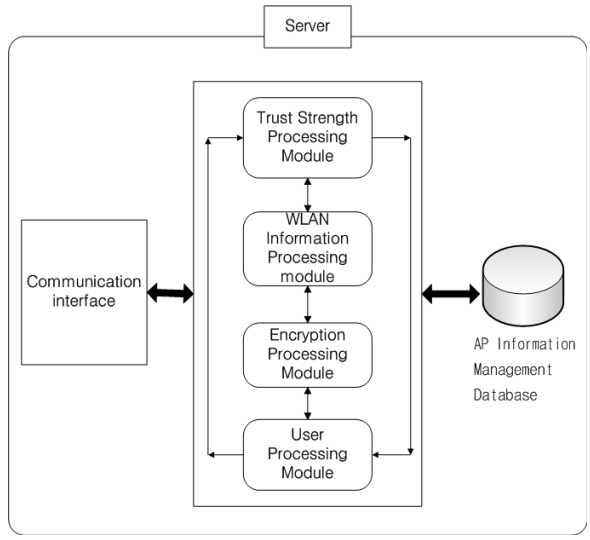


그림 3. 무선랜 정보 공유 서버 시스템 구조도
Fig. 3. System of WLAN Access Sharing Server

하며 크게 안드로이드 시스템 (WiFi, GPS, 무선랜 정보 관리 데이터베이스), 무선 정보 공유 모듈 (무선랜 등록 모듈, 암호화 처리 모듈, 위치 정보 모듈, 사용자 인증 모듈, 무선랜 정보 모듈), 사용자 인터페이스로 구성된다. 무선랜 등록 모듈은 사용자 등록을 위한 WiFi의 SSID, 보안키, GPS 좌표 정보를 무선랜 접근 공유 서버로 전송한다. 무선랜 등록 모듈은 사용자가 접속을 하기 위해 패스워드를 입력하면 패스워드를 따로 저장해서 가지고 있도록 한다. 무선랜 등록은 해당 무선랜의 접속이 완료된 경우에 가능하도록 한다. 위치 정보 모듈은 현재 GPS좌표를 나타내는 모듈이다. GPS를 실행시켜서 GPS좌표가 있으면 그대로 GPS좌표를 저장하고 있다가 위치 정보 모듈로 전송한다. 만약 GPS좌표를 일정시간동안 받아오지 못하면 Network Provider에서 위치 정보를 가져온다. 이 두 가지 방법이 모두 통하지 않을 경우, 안드로이드에서는 최근에 사용한 위치정보를 알아낼 수 있는 API 가 제공되는데 이 API를 이용해서 위치정보를 가져온다. 무선랜 정보 모듈은 안드로이드 내부 데이터베이스인 무선랜 정보 관리 데이터베이스 생성과 테이블의 생성 및 서버와의 동기화를 관리한다. 사용자 인증 모듈은 SNS 신뢰강도 기반의 무선랜 접근 공유 시스템을 사용하는데 필요한 인증의 정보를 디바이스에서 추출하여 서버에 등록하는 모듈이다. 암호화 처리 모듈은 위치 정보 데이터를 보호하기 위한 처리 모듈이다.

2.2.2. 무선랜 정보 공유 서버 시스템 구조

무선랜 접근 공유 서버 구조는 크게 통신 인터페이스와 데이터베이스의 정보를 처리하는 모듈(신뢰강도 처리 모듈, 무선랜 정보 처리 모듈, 암호화 처리 모듈, 사용자 처리 모듈) 그리고 관계형 데이터베이스인 AP 정보 관리 데이터베이스로 이루어진다. 통신 인터페이스는 무선랜 접근 공유 클라이언트와 무선랜 접근 공유 서버 간의 메시지 전송을 관리한다. 신뢰강도 처리 모듈은 무선랜 접근 공유 클라이언트에서 요청하는 사용자 정보를 이용해서 AP 정보 관리 데이터베이스를 검색하여 신뢰강도 정보를 전달하는 모델이다. 신뢰강도를 만족하는 사용자 정보는 무선랜 정보 처리 모듈로 전달된다. 무선랜 정보 처리 모듈은 신뢰강도 검색이 완료되면 무선랜에 대한 정보를 정리하고 데이터를 구조화한다. 암호화 처리 모듈은 무선랜 등록 정보의 데이터 보호에 중점을 두고 있다. 암호화는 AES를 기반으로 하며 전송은 HTTP를 이용한다. 사용자 처리 모듈은 신뢰강도 정보와 무선랜 정보 처리 모듈에서 받은 무선랜 정보를 관리하는 모듈이다. AP 정보 관리 데이터베이스는 사용자와 무선랜 정보를 관리한다. 암호화 처리 모듈로부터 전달받은 무선랜 등록 정보를 무선랜 정보 관리 데이터베이스에 저장한다.

Ⅲ. 구현 및 결과

3.1. 구현 환경

표 2와 표 3은 안드로이드 기반의 클라이언트와 웹 기반의 서버 시스템의 구현환경을 보여준다. 안드로이드 기반의 무선랜 접근 공유 클라이언트의 개발환경은 표 2와 같으며, 무선랜 접근 공유 서버의

개발 환경은 표 3과 같으며, 시스템 구성을 그림 4와 같다.

안드로이드 기반의 클라이언트에는 개발된 클라이언트 어플리케이션을 설치하였고, AP1과 AP2의 인증 메커니즘은 WPA2 PSK으로 변경 설정하였다.

표 2. 클라이언트 구현환경
Table 2. Development environment of Client

Domain	Version
Mobile OS	Android 2.2
Test device	Samsung SHW-M110S
Development OS	Windows 7 Enterprise K SP1
Development tool	Eclipse IDE

표 3. 서버 구현환경
Table 3. Development environment of server

Domain	Version
OS	Ubuntu 9.10 (Linux)
Web server	Apache 2.2.12
Server-side language	PHP 5.3.5
DBMS	Mysql 5.1.37
JAVA	1.6.0.24

3.2. SNS 신뢰강도 기반 무선랜 정보 공유 서비스 시나리오

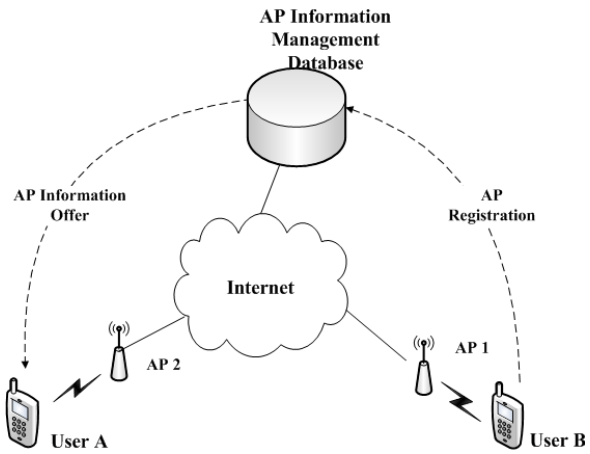


그림 4. 무선랜 정보 공유 시스템 구성 및 시나리오
Fig. 4. Scenario of SNS-based WLAN access sharing service

그림 4는 무선랜 정보 공유 시스템 구성 및 시나리오를 보여준다. 구현된 클라이언트와 서버의 동작을 검증하기 위해 다음과 같은 시나리오로 성능을 분석하였다.

먼저, 사용자 A와 사용자 B의 안드로이드 스마트 이동 단말에서 설치된 어플리케이션을 실행하고, 사용자 B (User B)는 무선랜 (AP1)을 AP 정보관리 데이터베이스에 무선랜 등록 과정을 거쳐 저장하게 된다. 등록과정에서 사용자 B는 AP1에 대한 신뢰강도를 1로 지정하여 저장하게 된다. 이후, 사용자 A (User A)는 또한 사용자 B와 동일한 과정을 통해 AP2에 대해 AP 정보 관리 데이터베이스에 등록하게 된다. 이후 사용자 A는 AP1의 무선 전송 범위로 이동하고, AP1의 접속을 시도하게 된다. 접속 시도 시, 사용자 A와 사용자 B가 AP1과 AP2를 공유하기 위해 사용자 A는 사용자 B로 무선랜 공유 요청 메시지가 AP 정보 관리 데이터베이스를 통해 전송하게 되며, 사용자 B는 이 메시지를 수신 한 후, 공유 여부를 결정하게 된다. 공유 동의 여부에 대한 응답 메시지는 AP 정보 관리 데이터베이스를 통해 사용자 A에게 전송된다. 만약 동의 하였다면, AP 정보 관리 데이터베이스로부터 AP1의 접속 정보를 획득하게 된다. 이후 사용자 A가 언제나 AP1에 다른 절차 없이 접속할 수 있게 된다.

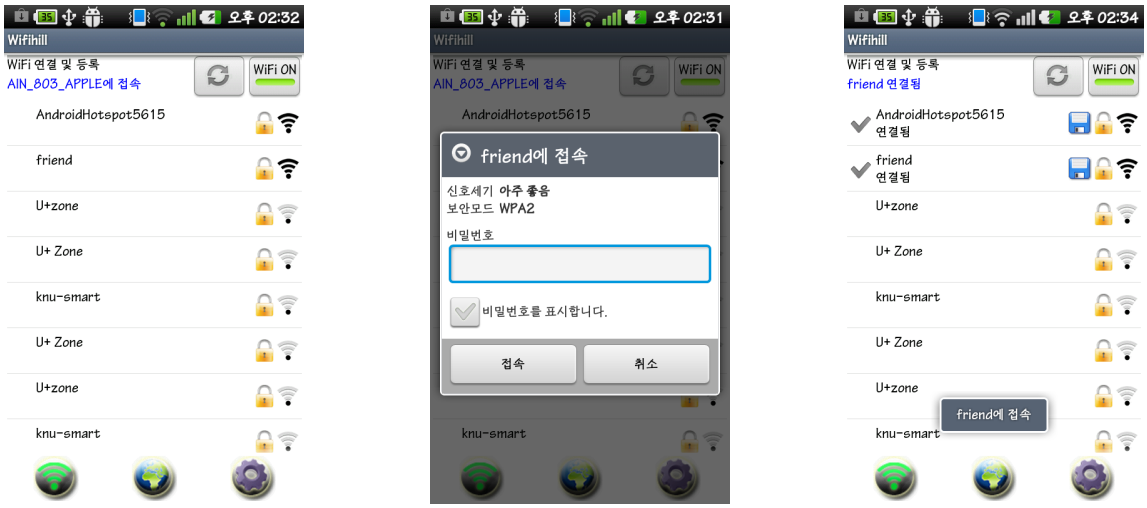
3.3. 구현 결과

3.3.1. 무선랜 정보 공유 클라이언트 구현

그림 5(a), (b), (c)는 무선랜 등록 과정을 보여준다. 그림 5(a)에서 사용자 A의 AP가 “friend”인 WPA2로 인증되어 있는 무선 AP를 검색한 화면을 나타낸다. AP friend는 AP 정보 관리 데이터베이스에 등록한다. 이후 사용자 B는 그림 5(b)에 보이는 것과 같이 AP friend를 저장 및 접속하게 된다. 이 접속 정보는 AP 정보관리 데이터베이스와 사용자의 스마트 이동단말의 무선랜 정보관리 데이터베이스에 저장된다. 5(c)는 사용자 B가 AP friend에 접속한 후의 화면이다. 이후 등록한 사용자는 이전에 저장해 놓은 보안키를 입력하지 않고 접속할 수 있다.
이후 다른 스마트 이동 단말에서 SSID가 friend인 AP가 검색되면 등록된 사용자에게 친구 요청 메시지를 송신하게 된다. 친구 요청 및 승인 과정을 통해 새로운 사용자는 등록된 AP를 공유하게 할 수 있게 된다.

3.3.2. 무선랜 정보 공유 서버 구현

신뢰강도 기반의 무선랜 공유 서비스 서버 데이터베이스 구조를 나타낸 그림이다. 본 관계형 데이터베



(a) (b) (c)

그림 5. 무선랜 접속 과정 화면 및 접속 화면
Fig. 5. Display view on WLAN access process of WLAN connection

이스는 크게 8개의 테이블로 구성되며 보안키의 공유가 필요없는 공개된 무선랜 경우에는 독립된 테이블로 존재한다. 보안이 설정된 무선랜 경우에는 APLIST_SECURE 테이블에 저장되며 APLIST_SECURE 테이블과 USER 테이블 사이에는 APUSE 테이블이 존재한다. APUSE 테이블은 어떤 사용자가 어떤 무선랜을 사용할 수 있는지를 나타내며 무선랜의 BSSID와 user_id, 사용자에게 공유된 날짜와 현재 클라이언트의 내부 데이터베이스와의 동기화 상태를 나타내는 DB_sync 속성으로 구성된다. APLIST_SECURE 테이블과 APUSE 테이블은 1:N의 관계로써 다수 사용자가 한 개의 무선랜을 사용할 수 있다. USER 테이블과 APUSE 테이블 또한 1:N 관계로써 한 사용자가 여러개의 무선랜을 사용

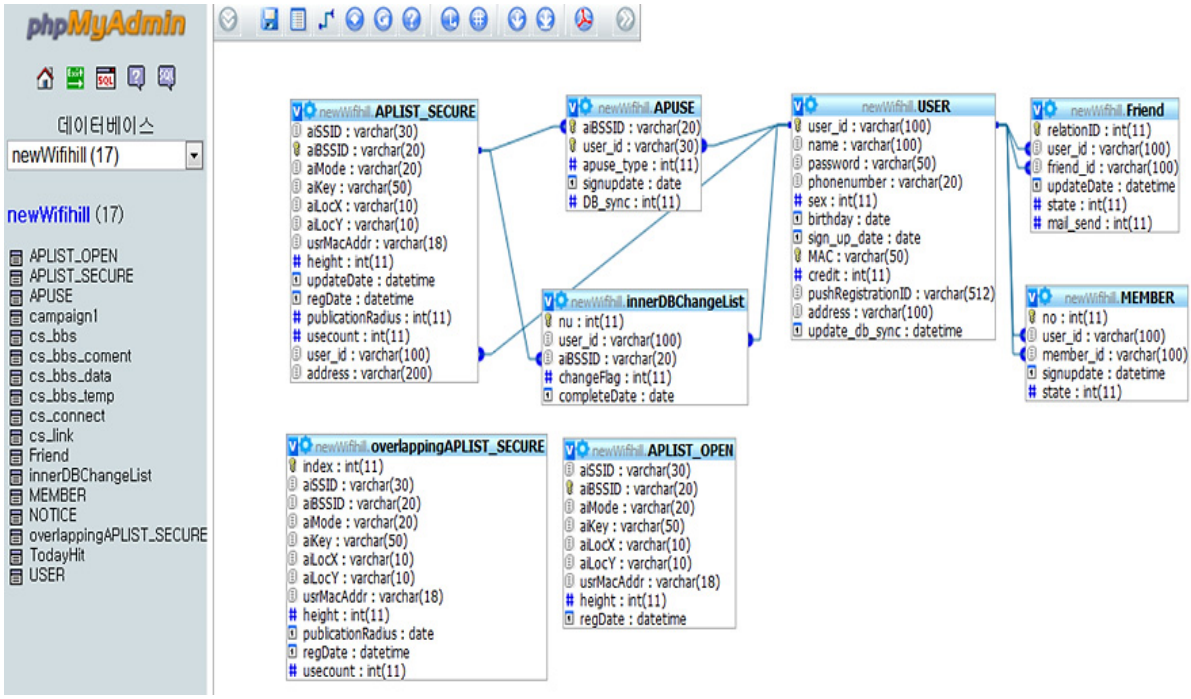


그림 6. 구현된 서버 시스템 데이터베이스의 구조 맵 화면
Fig. 6. Realized structure map of server system database and administrator's screen

할 수 있다. APUSE 테이블의 aiBSSID와 user_id 둘 다 같은 레코드는 APUSE 테이블에 존재하지 않으며 USER 테이블의 phonenumber와 mobile_mac_address도 후보키로써 USER 테이블 내에서 동일한 값은 존재하지 않는다.FRIEND 테이블은 신뢰거리가 가장 가까운 친구 관계만 나타낸 테이블이며 신뢰강도별 친구 관계는 FRIEND테이블을 사용하여 다음 절의 알고리즘을 통해 알 수 있다. relationID, user_id, friend_id, regdate, state, trust_class 속성을 가지고 있다. USER 테이블은 각 사용자의 정보를 저장하며 시스템 구현에 따라 속성이 추가되거나 삭제 될 수도 있지만 필수적으로 trust_strength는 추가되어야 한다. trust_strength는 사용자가 설정한 신뢰강도이며 자신이 설정한 신뢰강도를 만족하는 사용자에게만 자신의 무선랜 접속 정보를 공유한다.

Ⅳ. 결 론

본 논문에서 제안한 신뢰강도 기반의 무선랜 정보 공유 시스템은 자신의 무선랜의 보안은 그대로 사용하면서 친구들과 무선랜 보안키 노출의 위험 없이 무선랜을 안전하게 공유한다. 특히 클라이언트 측에서는 기존 안드로이드 설정창의 무선랜 접속기능을 전부 포함하였으며 자신의 친구들을 무선랜으로 부터 보안키를 공유 받음으로써 기존의 기능은 그대로 쓰면서 접속 가능한 무선랜은 대폭 증가하도록 하였다. 그리고 서버 측에서는 관계형 데이터베이스 관리 시스템을 사용하여 친구관계를 효율적으로 관리하였다. 사업자들은 무선랜의 인증을 중앙집중식으로 바꾼 서비스를 제공하고 있다. 하지만 무선랜을 설치해 놓은 곳의 무선랜만 사용할 수 있으며, 개인이 설치한 수많은 무선랜을 사용할 수 없다는 문제점이 있다. 본 논문에서 제안한 신뢰강도 기반의 무선랜 공유 시스템은 각 사용자들의 무선랜 보안과 공유를 함께 사용할 수 있도록 도와준다. 본 논문에서 제안한 신뢰강도 기반의 무선랜 정보 공유 시스템를 확장한다면 고효율의 네트워크망을 구축할 수 있을 것이다.

References

[1] J.H. Yoon, “WLAN Security Protocol”, Kyohaksa, 2005.

[2] Y.W. Park, “Issue and Implication of WLAN Market”, KISDI, 14(8), May 2002.

[3] Socialbakers Wdb Site, Nov, 201, http://www.socialbakers.com.

[4] K. Chard, S. Caton, O. Rana, K. Bubendorfe, “Social Cloud: Cloud Computing in Social Networks“, *IEEE International Conference on Cloud Computing*, pp. 99-106, 2010.

[5] Fon Web Site, No, 2011, http://corp.fon.com/en/this-is-fon.

우 연 경 (Yeon-Kyung Woo)

2011년 2월 영남대학교 전자공학과(공학사)
2012년~현재 경북대학교 전자전기컴퓨터공학과(공학석사)
<관심분야> U-healthcare network, Wireless body area network, HL7, IEEE 11073, Network management, Wireless communication

최 준 혁 (Jun-Hyuk Choi)

2010년 2월 경북대학교 전자공학과(공학사)
2012년 2월 경북대학교 전자전기컴퓨터공학과(공학석사)
<관심분야> U-healthcare network, Wireless body area network, HL7, IEEE 11073, Network management, Wireless communication

박 종 태 (Jong-Tae Park)

1978년 2월 경북대학교 전자공학과(공학사)
1981년 2월 서울대학교 전자공학과(공학석사)
1987년 8월 Univ. of Michigan EECS(공학박사)
1989년~현재 경북대학교 전자공학과 교수
2000년~2003년 IEEE Technical Committee on Information Infrastructure(TCII) 의장
1988년~1989년 삼성전자 컴퓨터시스템 사업부 수석연구원
1987년~1988년 미국 AT&T Bell 연구소 연구위원
1984년~1987년 미국 CITI 연구원
<관심분야> 이동통신, 모바일, 차세대 통신망운용, 네트워크 보안, 헬스케어 서비스