ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

iBeacon을 이용한 AP 자동접속 방안☆

An Automatic AP Connections Scheme using iBeacon

남 춘 성[1] 신 동 렬[1*]
ChoonSung Nam DongRyeol Shin

요 약

스마트 디바이스를 이용하여 특정 공간에서 미리 설정된 무선랜에 접속하는 방법은 개방형 방식과 사용자 인증 방식으로 나뉠 수 있다. 개방형 방식은 무선랜 접속을 위한 인증이 없이 접속하는 방법이다. 스마트 디바이스 사용자가 자신이 사용하려는 무선랜에 대한 정보를 SSID(Service Set IDentifier)를 통해 공공 무선랜 표기 형식에 따라 제공받아야 하지만, 모든 개방형 무선랜이 이러한 방식을 수동으로 입력하는 방식에는 무리가 있다. 반면에 사용자 인증 방식은 SSID와 PW(PassWord) 설정을 통해 사용자에게 무선랜 접속을 제공하는 방식이다. 따라서 SSID를 통해 공공 무선랜 표기 형식을 따를 수는 있지만, AP 접속을 위해서는 일일이 사용자가 수동으로 패스워드 입력을 통해 AP에 접속해야만 한다. 따라서 본 논문에서는 사용자 인증방식과 공공 무선랜 표기형식을 iBeacon 메시지 수신을 통해 자동적으로 AP에 접속할 수 있는 방안을 제안한다.

☞ 주제어 : 자동 접속, Access point, 공공 무선랜, SSID, Beacon, 안드로이드

ABSTRACT

There are two kinds of wireless network access to a certain place by using smart devices – 1) open (anonymous) - access and 2) user-authorized access. The open-access is a non-authorization connection method which does not need to require Smart device's user authorized information. It means open-access use only user's SSID (Service Set Identifier) information to access the wireless AP devices following public wireless network standard. This access mechanism is not suitable to use all of public wireless networks because users have to get all wireless network information around them. As a result, huge data for smart devices should be one of the most critical overload problems for them. Secondly, the user-authorized access method uses wireless network information (SSID and password) chosen by the users. So, the users have to remember and use the network access information data manually whenever accessing the network. Like open-access, this access method also has the operational and inconvenient problem for the users – manually inputting access information whenever connecting to the network. To overcome this problem in both schemes, we propose two improved wireless network access methods: 1) the implementation of automatic AP connection mechanism using user-authorization and iBeacon messages, and 2) SSID registration form for public wireless networks.

☞ keyword : Autonomous access, Access point, Public wireless LAN, SSID, iBeacon, Android

1. 서 론

2006년 애플사의 아이폰(iPhone) 출시를 기점으로 스마트폰에 대한 폭발적인 관심이 증가하였다. 대한민국의 스마트폰 보급률은 2015년 3월 기준 83.3%에 달할 정도로 높고 세계 4위의 보급률을 보이고 있다. 또한 전 세계적으로도 56개국 성인 인구의 스마트폰 보급률은 평균 약 60%에 이를 만큼 스마트폰은 이제 일반적인 모바일 통신 기기로서의 중추적 역할을 하고 있다[1]. 스마트폰의 증가는 기존의 PC(Personal Computer)를 기반으로 한 인터넷(Internet) 접속 형태에서 스마트 디바이스로 이전하는데 중추적인 역할을 하고 있다[2]. 모바일 인터넷 접속을 위해 사용자가 인터넷에 접속하는 방법은 LTE의 보급으로 인해 이동통신을 이용하여 접속하는 형태가 증가하였다. 하지만(2013년 62.5%, 2014년 86.9%), 여전히 무선랜(Wireless LAN)을 통한 인터넷 접속(2013년 78.7%, 2014년 83.7%)이 모바일 인터넷 접속에 상당 부분을 차지하고 있다[3]. 특히, 평균적으로 60분 이상을 인터넷에 접속해서 사용하는 비율은 74.4%로 스마트 디바이스를 사용하는 사용자 대부분이 무선랜을 통한 접속 방식을 사용하고 있다.

1 College of Information and Communication Engineering, SungKyunKwan University, Suwon, 440-746, Korea.
* Corresponding author (drshin@skku.edu)
[Received 15 March 2016, Reviewed 26 March 2016(R2 7 August 2016, R3 22 November 2016), Accepted 5 January 2017]
☆ 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2016R1A6A3A11932892)

스마트 디바이스 사용자가 무선랜을 통해 인터넷을 연결하기 위해서는 통신사에서 제공하는 공공랜 서비스 인증 방식을 통해서 접속해야 한다. 공공랜 서비스를 인증하기 위한 방식은 이동통신사를 기반으로 대표적으로 SMS(Short Message Service)을 통해 사용자를 인증방식으로 가입된 기존 이동통신사의 정보를 이용하는 방식이다. 또한, EAP-AKA(Entensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement)**[4] 방**식은 이동통신사에서 제공한 USIM(Universal Subscribe Identity Module) 정보를 이용하여 자동접속과 암호화키를 제공하여 무선랜에 접속하는 방식이다[5]. 하지만, 일반적으로 통신사의 인증을 거치지 않고 무선랜을 제공하는 가정, 가게, 공공기관들 등은 무선랜 인증을 위해 통신사 인증 방식을 통해서 운영자가 직접 SSID(Service Set IDentifier) 설정 및 비밀번호 설정을 각각 해줘야한다. 따라서 대부분의 가정, 가게, 기관과 같은 장소에서는 무선 접속을 위한 AP(Access Point)에 사용자 인증 방식을 통해서 접속을 허용하는 형태로 구성되어 있다. 즉, 개인적인 공간에서 사용하는 무선랜의 경우 접속되는 단말의 이용자와 대수를 파악할 수 있기 때문에 사용자 인증 방식을 통한 접속에 무리가 없다. 하지만 공공기관 혹은 특정 공간에서의 불특정 다수에게 무선랜 접속을 허용하기 위해서는 직접 사용자 인증을 위한 아이디(ID)나 패스워드(password)를 알려줘야 하는 불편함을 가지고 있다. 이를 위해 특정 공간에 Wi-Fi접속을 위한 패스워드를 적어놓는다던가, 영수증에 패스워드를 출력해서 인지해 준다거나, 혹은 직접 무선랜을 담당하는 관리자에게 직접 물어서 이를 파악하는 등 사용자가 직접적인 행동에 의해서 접속 방안을 해결해야만 한다. 또한 개방형 방식으로 무선랜을 설정하는 경우라 하더라도 무선랜 접속을 위해 관리자 혹은 사용자가 일일이 표준화된 공공랜 SSID에 따라 SSID를 설정하고 적용해야 하므로 이를 위한 추가적인 작업이 필요하다.

따라서 본 논문에서는 스마트폰 사용자가 특정 공간에 설치된 무선랜에 접속하려 할 때 기존의 개방형 방식과 사용자 인증 방식에 관계없이 iBeacon을 이용하여 두 가지 방식을 지원하는 방안을 제안한다. 이를 위해 본 논문에서는 iBeacon의 페이로드(payload)값을 이용하여 사용자 인증 암호 및 공공 무선랜의 SSID 표기방식을 지원하기 위한 시스템을 구축하였다.

본 논문의 2장에서는 관련연구를 통해 공공 무선랜 서비스 제공방안을 위한 SSID 표기 방식 표준과 무선랜 사용 방식에 따른 장단점을 파악하였다. 또한, iBeacon의 메시지 형태와 운영 방식을 서술하였다. 3장에서는 iBeacon을 이용하여 AP에 자동 접속할 수 있는 방안을 SSID를 공개된 상태에서 앱(App)에서 처리하는 경우와 특정 서버를 통해 제공하는 경우를 기반으로 구성하였다. 4장에서는 구현된 스마트 디바이스용 앱과 구현 방식에 대해서 설명한다. 5장에서는 결론을 맺는다.

2. 관련 연구

2.1 공공 무선랜 서비스 제공시 SSID 표기

공공용 무선 랜 서비스를 제공하기 위해서는 TTA에서 표준화한 지침[6]을 기반으로 운영되어야만 한다. 공공용 무선랜 서비스 제공을 위해서는 사용자 편의성 측면과 정보보안 측면을 적절히 조화하는 방식이 필요하다. 사용자 편의성 측면에서는 특별한 접근 암호를 가지지 않고 비보안 방식으로 무선랜에 접근하는 방식을 따라야 한다. 이와 같은 경우 초기 안내 페이지(보안관련)를 공지함으로써 사용자가 비보안 접속을 허용하는 것을 권고해야만 한다. 즉, 사용자가 초기 안내 페이지에 동의한 경우 사용자는 사용자 등록을 통해서 비보안 접속 공공랜에 접속을 통해 외부 인터넷과의 연동이 가능하다. 공용 무선랜 식별자를 제공하는 방법은 SSID를 0~32바이트 길이로 설정해야만 하고 이를 ASCII(American Standard Code for Information Interchange) 코드로 표기하여야 한다. 이는 각 무선랜을 제공하는 AP별로 네트워크 이름을 부여하는 것이 가능하기 때문이다. 공공 무선랜 SSID 표기 방식은 다음과 같이 공공기관 및 공공시설 등의 이름을 추가하여 표기할 수 있는 방식을 따른다. 이러한 표기 방식은 (표 1)과 같다.

(표 1) 공공 무선랜 SSID 표기방식
(Table 1) Public Wi-Fi SSID Expression

방식	내 용
단일표기 방식	'브랜드명' = PublicWiFi 및 PublicWiFiSecure
기본표기 방식	<SSID> = "PublicWiFi" + "@" + <제공주체>
확장표기 방식	<SSID> = "PublicWiFi" + "@" + <시설명> + "." + <제공주체>

위 (표 1)에서 <제공주체>는 지자체 및 공공기관 등의 명칭을 기입하게 되어 있고, <시설명>은 무선랜 핫스팟(hotspot)이 구축된 장소로 되어 있다. 이러한 공용 무선

랜의 경우에 SSID를 공개로 설정하여 무선 네트워크 검색을 가능하게 해야만 한다. 또한, SSID 표기방식에 의해서 사용자가 서비스 지역과 제공 시설에 대한인지를 가능하게 해야 하는데 그 목적을 갖는다.

따라서 무선랜을 제공하는 개인, 상점, 기관 등은 SSID 표기방식에 따라 공공 무선랜을 설정할 필요성이 있다 . 만약 무선랜의 이러한 설정 방식을 따르지 못 한다면 위와 같은 표기 방식을 이용한 무선랜 설정 방식은 사용할 필요가 없을 것이다. 이에 기존의 SSID 자체를 변경하지 않고 무선랜 AP 접속을 위한 사용자 인증을 제공해야만 한다. 이를 위해서는 AP 접속 과정을 통해서 표준화된 공공 무선랜 형식을 적용하고 사용자가 수동적인 인증 절차를 갖지 않으면서 자동적인 AP 접속이 가능한 방법을 찾는 것이 중요하다. 따라서 본 논문은 사용자 인증과 공공 무선랜 표기 방식을 수용하고 자동적으로 AP접속이 가능한 방안을 제시하였다.

2.2 무선랜 사용 방식

무선랜에 접속하는 기술은 통신사를 통해 제공되거나 개인 혹은 공공기관에서 무료로 서비스 제공을 위한 무선 접속방식으로 이루어져 있다. 또한, 이동통신 기술에 비해 고속의 무선접속을 가능하고 비면허 주파수를 사용하여 누구나 구축 및 서비스 제공이 가능한 방식이다. 무선랜 사용 방식은 접속 방식에 따라 3가지로 분류될 수 있다. 첫째, 개방형 방식으로 무선랜 AP에 접속한 모든 단말에게 IP를 할당해 주는 방식으로 별도의 사용자 인증 및 데이터 암호화가 필요 없는 방식이다. 이와 같은 경우 무선랜을 접속하기 위한 스마트 디바이스는 단지 SSID를 통해 무선랜이 존재하는 것을 인지하기 때문에 단지 사용자의 선택에 의해서 접속할 수 있는 형태이다. 이러한 방식은 공공 무선랜과 같은 표준을 따르지 않기 때문에 사용자가 접속하는 공간과 제공자에 대한 정보는 단지 SSID를 통해 수신할 수밖에 없다. 둘째, 사용자 인증 방식이다. 사용자 인증 방식은 인증서, 아이디/비밀번호, 단말 MAC 주소 등 다양한 방식으로 AP의 접속을 제한하는 방식이다. 일반적으로 사용자가 AP에 접속하기 위한 SSID를 수신 한 후에 이에 맞는 비밀번호를 입력하여 접근하는 방식이다. 사용자는 접속을 위해서 반드시 비밀번호를 알아야만 한다. 하지만 제공된 SSID의 비밀번호를 알아내기 위해서는 사용자가 직접 무선랜을 설치한 관리자로부터 정보제공을 받아야만 가능하다. 이를 위해 관리자는 비밀번호를 물품의 영수증 혹은 별도의 공지를 통해 정보를 제공해야 하는 추가적인 과정이 필요하다. 특히, 제공된 패스워드가 주기적으로 변경될 경우에는 이러한 과정을 반복해야만 한다. 셋째, 데이터 암호화 방식이다. 데이터 암호화 방식은 기존 AP와 단말에 고정형 암호키를 동일하게 설정하는 방식이다. 이는 개인 혹은 공공기관에서 불특정 다수에게 무선랜을 제공하기 위해서는 고정형 암호를 노출시켜야만 한다. 따라서 일반적으로 공공 무선랜 구축을 통해 사용자 접속을 인증하기 위한 방법으로는 적합하지 못 한다[5].

따라서 본 논문에서는 iBeacon을 이용하여 개방형 방식에서는 SSID를 표준 표기 방식으로 자동 전환하여 제공하는 방법과 사용자 인증을 대체하기 위한 방안을 제시한다.

2.3 iBeacon

iBeacon은 애플사에서 실내위치 측정을 위한 기술로 발표되었다. iBeacon을 이용하기 위해서는 BLE(Bluetooth 4.0 이상)를 통한 메시지 송수신이 가능해야만 한다. BLE는 접속을 허용하지 않는 Advertisement 패킷 전송을 통해 이루어지기 때문에 매우 적은 통신비용과 에너지 소모를 갖는다. 특정한 접속을 허용하지 않기 때문에 iBeacon 디바이스는 브로드캐스팅(broadcasting)방식으로 데이터를 전송한다. iBeacon의 패킷은 Bluetooth 패킷의 데이터 포맷과 같으며, 총 47Bytes로 되어 있다. 데이터 포맷 안의 Payload에는 iBeacon Prefix(9bytes) UUID(Universal Unique ID, 16bytes), Major(2bytes), Minor(2bytes) 그리고 TX Power(2bytes) 값이 있다. iBeacon Prefix는 Advertising flags(3bytes), Advertising Header(2bytes), iBacon Type(1byte), iBeacon Length(1byte)로 설정되어 고정되어 있다. 비콘 제조사가 iBeacon규격을 따르지 않는다면 수정도 가능하다. UUID는 iBeacon을 식별하는 제품 고유의 ID이다. 따라서 UUID를 이용하여 각 iBeacon 디바이스를 구분할 수 있다. Major와 Minor는 iBeacon을 식별하는데 추가적인 요소로 사용된다. 그리고 TX Power은 iBeacon 디바이스가 메시지를 브로드캐스팅 하는 파워를 의미하며, 거리 값을 계산되는데 사용한다. 이 값과 수신된 RSSI(Received Signal Strength Indication)값에 의해서 iBeacon은 거리를 식별한다. iBeacon의 영역은 거리에 따라 Immediate, Near, Far로 구별할 수 있다[7,8].

위 정의된 iBeacon의 데이터 중에서 Major와 Minor값은 iBeacon을 식별하거나 개발자가 추가적으로 임의로 사용할 수 있는 값이다. 따라서 위 두 값을 이용해서 공공 SSID 표시와 사용자 인증을 위해 사용될 수 있다.

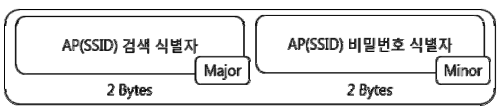
3. iBeacon이용 AP 자동접속 방안

iBeacon의 메시지를 이용하여 AP의 SSID와 패스워드를 제공하기 위해서는 iBeacon의 메시지가 이를 표현해야만 한다. 기본적으로 iBeacon에서 SSID를 대체할 수 있는 데이터의 크기가 Major 및 Minor 각 2bytes씩 4bytes로 밖에 표현할 수 없다. 따라서 공공랜을 위한 SSID를 생성하기 위해서는 AP접속을 위해 스마트 디바이스 어플리케이션에서 직접 SSID를 저장하여 제공된 Major값과 일치하는 지를 판단해야만 한다. 또 다른 방법으로는 Major, Minor값에 의해서 SSID와 패스워드를 관리하는 서버를 통해 사용자가 매번 접속정보를 받아와야만 한다. 따라서 본 논문에서 iBeacon을 이용하여 AP에 자동접속하기 위한 방안은 SSID와 패스워드를 직접 스마트 디바이스의 어플리케이션에서 선택 혹은 검출하는 경우와 외부 서버로부터 이를 수신 하는 방법 두 가지로 설계할 수 있다.

3.1 AP의 SSID와 패스워드를 앱에서 검출

3.1.1 앱을 통한 관리자 SSID/PW 설정 방법

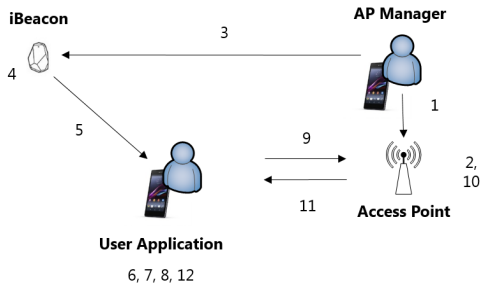
iBeacon에 메시지 중에서 사용자 혹은 개발자가 임의로 데이터를 변경해서 사용할 수 있는 것은 Payload의 **Major, Minor** 값이다. 이는 임의로 서비스에 맞게 변경될 수 있다. 따라서 본 논문에서 Major와 Minor값을 기반으로 AP에 접속하기 위한 방안으로 이 두 데이터를 (그림 1)과 같이 설정할 수 있다.



(그림 1) iBeacon의 Major 및 Minor 데이터 포맷 정의
(Figure 1) Major and Minor data format of iBeacon

(그림 1)과 같이 iBeacon의 메시지를 사용하게 되면 AP를 관리하는 관리자는 AP의 SSID와 PW를 각 2bytes씩으로 AP를 설정할 수 있다. 관리자는 AP에 접속하여 각각을 설정하고 난 후에 AP에 SSID와 PW를 설정한 값 그대로 iBeacon에 접속하여 이를 Major와 Minor 값으로 설정할 수 있다. 이 과정은 (그림 2)의 (1)과 (2)과정이고, (표 2)에서 자세히 설명되어 있다.

(표 2)에서 4번과 5번은 iBeacon에서 직접적으로 Major와 Minor값을 재설정하여 주위 사용자 디바이스에게 BLE형태로 데이터를 브로드캐스팅하는 것을 설명한다.



(그림 2) iBeacon에 의한 자동 접속 방안 1 - 앱
(Figure 2) Automatic AP access by iBeacon 1 - Smart device App

(표 2) iBeacon에 의한 AP 자동 접속 순서 - App
(Table 2) Automatic AP access order by iBeacon - App

번호	내 용
1	AP의 SSID 및 PW 설정
2	AP 재설정
3	Major(SSID), Minor(PW) 등록
4	iBeacon message 재설정(Major, Minor)
5	iBeacon message 전송
6	iBeacon Message 수신 및 식별
7	앱에서 Major(SSID), Minor(PW) 추출
8	SSID를 미리 설정한 공용 무선랜 SSID와 매칭
9	추출된 Major(SSID)와 Minor(PW)를 이용하여 AP에 접속 시도
10	사용자 디바이스 접속 인증
11	접속 IP 할당
12	AP 접속 완료

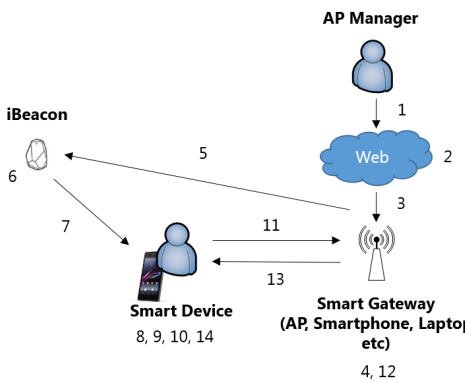
사용자가 (표 2)의 6번과 같이 메시지를 수신하면, 메시지를 추출하고(7번), 기존에 설치된 앱에서 Major값으로 설정한 공공 무선랜 SSID를 찾아 사용자에게 보여주고, 또한 Minor값으로 설정한 PW를 앱에서 찾아 AP접속을 위한 정보로 사용할 수 있다. (표 2)의 9번에서 사용자 스마트 디바이스는 추출된 SSID와 PW정보를 통해 AP에 접속을 요청할 수 있다. 이를 수신한 AP는 접속 인증과 할당을 통해서 외부 인터넷과의 연결을 허용할 수 있다.

3.1.2 웹을 통한 관리자 SSID/PW 설정 방법

iBeacon과 같이 블루투스 장비들은 기기 자체의 저전력 기능과 위치 서비스만을 위한 장비이기 때문에 웹 접근을 위한 추가적인 장비가 장착되어 있지 않다. 사용자가 외부에서 iBeacon을 웹으로 연결하여 설정 및 관리하

기 위해서는 스마트 게이트웨이(smart gateway)[9]가 필요하다. 또한, 사용자가 특별한 어플리케이션을 통해서가 아니라 일반적인 웹 프로토콜과 언어(HTML, Javascript, PHP, SCC 등)를 활용해 사물의 기능과 데이터 접근을 가능하게 할 수 있는 WoT(Web of Things)를 이용할 필요가 있다[10]. 따라서 본 논문에서는 iBeacon의 SSID 및 PW 정보를 외부에서 설정 하고 운영하는 방법으로 WoT를 이용하여 이를 설정하였다. 스마트 게이트웨이와 통신할 수 있는 방법은 JSON(JavaScript Object Notation)[11]를 이용하여 설정하였고, 데이터 형식은 다음 같이 설정하였다.

```
Server: autowifi.com
Date: Mon, 07 Jan 2016 09:38:06 GMT
Content-Type: application/json; charset=utf-8
Status: 200 OK
{
        "ssid": "PublicWiFi@skku.nrlab",
        "password": "534f4b4354 ",
        "major": 29572,
        "minor": 12595
}
```



(그림 3) iBeacon에 의한 자동 접속 방안 2 - Web
(Figure 3) Automatic AP access by iBeacon 2 - Web

이러한 데이터 형식을 이용하여 사용자는 웹 프로토콜과 스마트 게이트웨이를 통해 iBeacon의 Major(SSID) 및 Minor(PW) 값 설정을 스마트 게이트웨이로 요청할 수 있다. 이는 (그림 3)의 (1),(2),(3)을 통해 표시되어 있고, (표 3)에서와 같이 설명되어 있다. 즉, (그림 3)의 (1)에서 사용자가 웹페이지를 통해 스마트 게이트웨이에 접속하여 웹페이지 상에서 사용자는 스마트 게이트웨이와 연관된 iBeacon을 선택하고 Major 및 Minor 설정한다. 이후 이러한 명령은 스마트 게이트웨이에 iBeacon 데이터(Major, Minor) 및 AP의 SSID/PW 변경 요청하는 것이다. (그림 3)의 (4)에서 스마트 게이트웨이가 접속된 AP, 스마트 디바이스, 노트북 등의 AP역할을 하는 디바이스의 SSID/PW 설정한다. 그리고 스마트 게이트웨이는 요청된 iBeacon에 연결하여 Major(SSID) 및 Minor(PW)를 변경한다. 이후의 과정은 3.1.1의 과정과 같다.

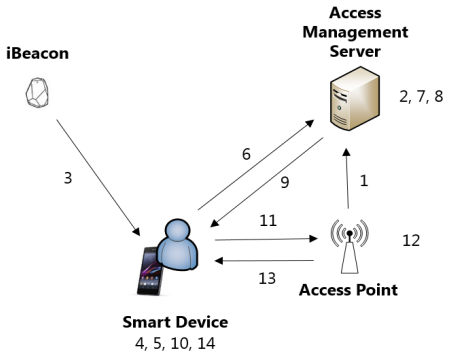
(표 3) iBeacon에 의한 AP 자동 접속 순서 - Web
(Table 3) Automatic AP access order by iBeacon - Web

번호	내 용
1	스마트 게이트웨이에 접속
2	iBeacon에 Major 및 Minor 설정
3	iBeacon 데이터(Major, Minor) 및 AP의 SSID/PW 변경 요청
4	AP역할을 하는 디바이스의 SSID/PW 설정
5	iBeacon Major(SSID), Minor(PW) 설정 요청
6	iBeacon Major(SSID), Minor(PW) 설정
7	iBeacon message 전송
8	iBeacon Message 수신 및 식별
9	앱에서 Major(SSID), Minor(PW) 추출
10	SSID를 미리 설정한 공용 무선랜 SSID와 매칭
11	추출된 Major(SSID)와 Minor(PW)를 이용하여 AP에 접속 시도
12	사용자 디바이스 접속 인증
13	접속 IP 할당
14	AP 접속 완료

3.2 AP의 SSID와 패스워드를 서버에서 수신

3.1의 방안에서 SSID와 PW를 앱(App)에서 결정하는 방법은 iBeacon를 수신시 변경되는 정보를 반영하기 어렵다. 즉, 앱의 지속적인 업그레이드를 통해서만이 가능하다. 따라서 SSID와 PW를 대표하는 Major 및 Minor값은 유지한 채 AP에 대한 접속 정보만을 제공할 수 있는 방안이 필요하다. 이를 위해서는 iBeacon의 메시지는 특정한 서버에 접속하기 위한 URL(Uniform Resource Locator)로 변경되어야만 한다. 하지만 Major 및 Minor의 데이터 길이가 4byte 밖에 되지 않기 때문에 일반적인 URL 주소로는 포함할 수 없다. 따라서 URL short link[12]를 이용하여

4bytes로 표현할 수 있는 주소러 변환해야 한다. 가령 “www.daum.net”은 12byte가 표현되지만 URL short address로는 ”WkNF“로 단지 4byte만으로 표현할 수 있다. 따라서 SSID와 PW를 제공하는 AMS(Access Management Server)의 URL를 4byte로 구성이 가능하다. 실제 URL Short link는 “http://goo.gol/####”과 같이 정형화된 주소는 앱에 저장하고 나머지 4byte(####)의 주소만을 iBeacon 메시지에 설정할 수 있다. 따라서 이와 같은 방법으로 iBeacon을 통해서 AMS에 접속하여 표면적으로 공개되지 않는 공공 무선랜의 SSID와 PW를 가져올 수 있다. 이는 (그림 4)와 (표 4)에서와 같이 나타낼 수 있다.



(그림 4) iBeacon에 의한 자동 접속 방안 3 - Server
(Figure 4) Automatic AP access by iBeacon 3 - Server

(표 4) iBeacon에 의한 AP 자동 접속 순서 - Server
(Table 4) Automatic AP access order by iBeacon - Server

번호	내 용
1	AP의 SSID 및 PW를 ACM에게 전송
2	설치된 iBeacon과 AP를 매칭
3	iBeacon message 전송
4	iBeacon message 식별
5	iBeacon Major 및 Minor 로 URL short link 생성
6	ACM에 iBeacon UUID 전송
7	iBeacon 설치된 AP의 SSID 및 PW 식별
8	공공 무선랜 식별자 생성
9	AP 인증 정보 전달(SSID, PW, 공공무선랜 형식)
10	SSID 매칭 및 PW 추출
11	매칭된 AP 접속
12	AP 접속 인증 확인
13	접속 IP 할당
14	AP 접속 완료

(그림 4)의 (1)에서 AP는 스마트 게이트웨이 혹은 관리자에 의해서 자신의 SSID와 PW를 ACM에 등록해야한다. 등록된 SSID와 PW는 AP의 위치와 사용용돈에 따라 공공 무선랜 형식의 SSID 정보를 제공한다. (그림 4)의 (2)는 AP가 설치된 곳의 iBeacon과 연관하여 데이터를 저장하여 추후에 iBeacon에 의해서 요청이 오면 AP의 접속 인증 정보를 전송한다. 사용자가 (그림 4)의 (3), (4), (5)에서 iBeacon 메시지를 수신 받으면, 이전과 같이 Major 및 Minor값을 추출하고 이를 통해 URL short link를 생성하여 ACM에게 접속한 AP의 인증 정보를 요청한다. ACM은 사용자가 수신한 iBeacon의 고유번호인 UUID를 구분한다. 이를 통해 접속할 수 있는 AP의 SSID와 PW를 검색하여 사용자에게 보내주면 사용자는 이전의 과정과 동일하게 AP에 접속할 수 있다.

제안된 방법들을 독립적인 앱으로 사용되기보다는 기존의 기업들이 제공하는 앱에 add-on하여 사용될 수 있는 기술로 무선랜의 위치와 용도 그리고 사업자를 사용자가 알 수 있도록 TTA의 공용 무선랜 표준 형식에 따라 SSID를 가상으로 설정할 수 있다. 또한, 사용자가 별다른 행동이나 명령 없이 단지 스마트 디바이스를 이용해서 서비스를 사용될 수밖에 없는 상황 즉, 상점에서 스마트 디바이스의 앱을 이용하는 경우[13,14]에서 자연스럽게 공공 무선랜에 접속할 수 있는 기술을 제공할 수 있다.

4. 제안한 시스템 구현 및 분석

4.1 개발 환경

본 논문에서 iBeacon 메시지를 통해 AP 접속을 위한 사용자 App과 사용자에게 AP 접속 정보를 제공하기 위한 서버를 구성해야만 한다. 이를 위한 시스템 개발환경은 (표 5)와 같은 환경에서 개발되었다.

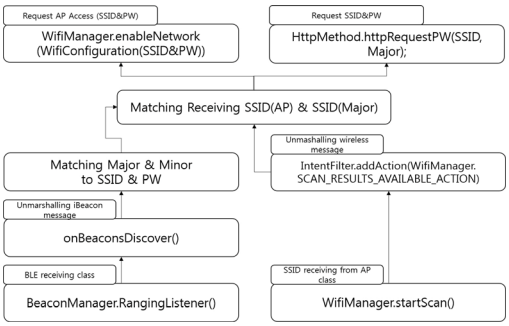
(표 5) 개발환경
(Table 5) Development environment

H/W	스마트 디바이스	서버 컴퓨터
Process (cpu)	SnapdragonTM 800 2.26GHz(Nexus 5)	Intel Core i7 2.3 GHz
Memory	2GB	8GB
OS	Android 5.0	Window 10 pro
Language	Java 1.8	Java 1.8
Framework	-	Apache Tomcat + Spring framework

4.2 iBeacon AP 자동 접속 구성도

4.2.1 사용자 App 의 구성도

iBeacon의 메시지를 처리하기 위한 사용자 App에서의 구성은 (그림 5)와 같다. (그림 5)에서 BLE를 수신하기 위해 BeaconManager.RangingListener()를 이용한다. 이를 통해 수신된 메시지는 onBeaconsDiscover()를 통해 메시지의 데이터 Major 및 Minor 값을 추출할 수 있다. 추출된 Major 및 Minor 값은 기존에 저장된 값을 통해 찾을 수 있다. 이를 통해 WifiManger.startScan()으로부터 수신된 WiFi의 SSID와 이름이 같은 AP에 WiFiManger.enable Netwok를 통해서 접속할 수 있다. 또한, AP의 SSID와 PW를 AMS로부터 수신 받는 경우에는 SSID와 PW를 통해 서버의 주소로 변경하고, 변경된 주소에 BLE의 iBeacon prefix값을 보내어서 현재 BLE와 연관된 AP의 정보를 요청할 수 있다. 이는 (그림 5)에서 HttpMethod.httpRequestPW (SSID,Major)를 통해 이루어진다. 또한, 이 과정은 위에서 설명한 AP접속을 위해 App에서 처리는 하는 방식과 Web를 통해 서버에서 처리하는 방식 두 가지 경우를 모두 포함한다.

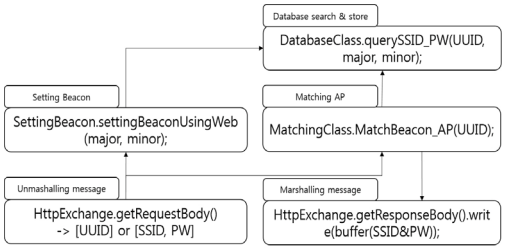


(그림 5) 사용자 App내 AP접속 처리 구성도
(Figure 5) AP access process in user device's app

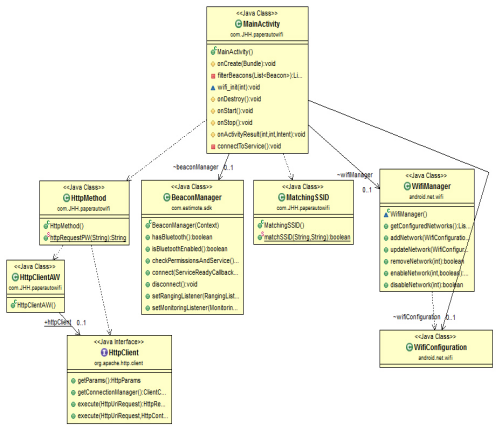
이와 같은 구성에 의한 구현된 클래스 다이어그램은 (그림 6)과 같다.

4.2.2 Server 구성도

iBeacon 메시지를 App안에 미리 설정된 값이 아닌 AMS 서버에서 iBeacon과 AP의 관계를 명시하고 관리하기 위한 방안을 위한 구성 (그림 7)과 같다. 그림에서 사용자 자신의 영역에서 자동적으로 선택된 iBeacon의 UUID를 AMS로 보내면 AMS는 HttpExchange.getRequest



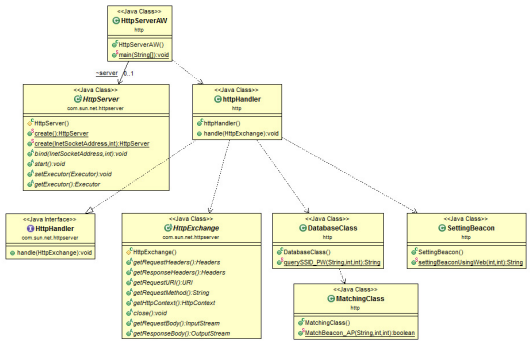
(그림 7) AMS를 통한 AP 접속 처리 구성도
(Figure 7) AP access process in AMS



(그림 6) 사용자 App내 AP접속 클래스 구조도
(Figure 6) Class diagram of AP access in user device's app

Body()에서 UUID를 추출한다. 이러한 UUID 는 자신과 연결된 AP를 찾아내기 위해서 MatchingClass.MatchBeacon. AP()로 넘겨지고 DatabaseClass.query()를 통해서 AP의 SSID와 PW를 찾아낸다. 연관된 SSID와 PW는 HttpExchange. getResponse Body().write()를 통해서 사용자 디바이스로 전송할 수 있다. 만약 관리자가 iBeacon과 AP의 연관 및 정보를 새롭게 설정한다면, 이전과정과 같이 데이터를 전송하되, UUID 뿐 아니라 SSID(Major), PW(Minor)를 AMS로 전송한다. 수신된 데이터를 기반으로 SettingBeacon. settingBeaconUsing Web()를 통해 iBeacon 값은 새롭게 설정할 수 있고, 이를 이전과 같이 Database Class.query SSID_PW()를 통해 등록하고 등록된 값을 MatchingClass. MatchBeacon_ AP()를 통해 AP와 다시 연동시킬 수 있다.

이와 같은 구성에 의한 구현된 클래스 다이어그램은 (그림 8)과 같이 구현하였다.

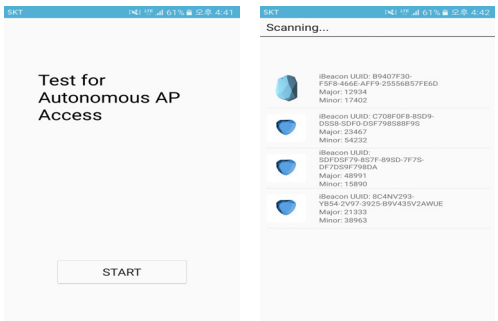


(그림 8) AMS내 AP접속 클래스 구조도
(Figure 8) Class diagram of AP access in AMS

4.3 iBeacon AP 자동 접속 App

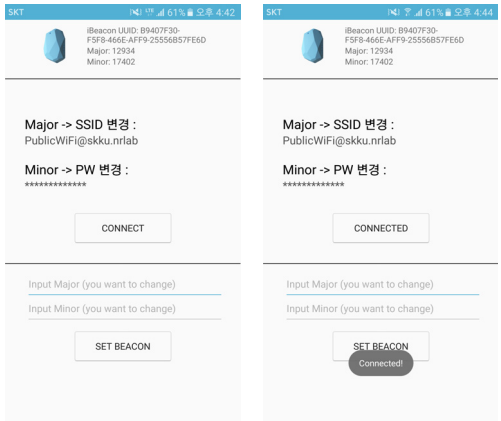
위에서 제안한 iBeacon을 이용한 AP 자동 접속 App은 기본적으로는 사용자가 작동하는 방법을 알 필요는 없다. App의 백그라운드에서 작동하여 사용자의 추가적인 작업 없이 AP에 접속해야만 한다. 하지만 iBeacon 메시지를 확인하고 AP 자동적인 접속을 확인하기 위해서는 각 단계별로 기능을 확인할 수 있도록 구현하여야만 한다. 따라서 본 논문에서는 이러한 과정을 담은 App을 구현하였다.

(그림 9)에서는 App의 메인페이지와 주위 iBeacon 디바이스를 찾는 과정을 보여준다. (그림 9)의 (2)에서와 같이, 앱이 작동하면 앱은 BLE를 송신하는 iBeacon 디바이스의 메시지를 수신하여 각 디바이스별 정보를 수신한다. UUID는 디바이스를 판단하기 위해서 각각 다른 값으로 변경하였다. 주어진 정보 중에서 SSID와 PW를 찾아내기 위해 Major 및 Minor 값을 따로 분류하여 나타내었다.



(1) (2)

(그림 9) iBeacon AP 자동 접속 App 초기 화면
(Figure 9) Main page & scanning page of autonomous AP App by iBeacon



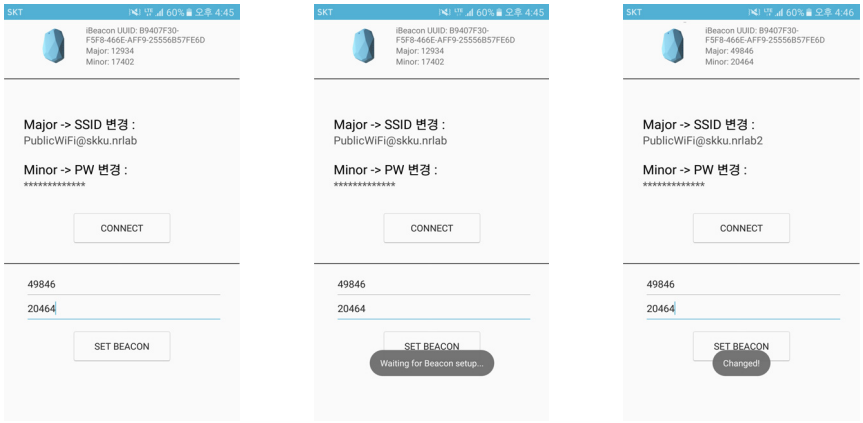
(1) (2)

(그림 10) App에서 SSID 및 PW 매칭
(Figure 10) Matching SSID and PW in App using by Major and Minor data

만약 위와 같은 iBeacon 중에서 (그림 9)의 (2)에서 첫 번째 iBeacon은 App에서 미리 지정된 SSID와 PW를 변경하는 방안이다. 이는 위의 과정에서 3.1의 과정과 같다. (그림 10)의 (1)에서 선택된 iBeacon의 메시지를 통해 SSID와 PW의 값으로 변경한 것을 알 수 있다. 이를 'CONNECT'버튼을 통해 AP에 접속을 요청하면 (그림 10)의 (2)와 같이 접속이 이루어지고 AP접속을 통해 디바이스는 WiFi 상태로 연결됨을 볼 수 있다. 이때, 접속되는 AP의 SSID(PublicWiFi@skku.nrlab)는 공공 무선랜 표기 방식으로 자동 변경됨을 볼 수 있다.

만약, 사용자가 지정된 iBeacon의 Major 및 Minor 값을 변경하여 새로운 AP에 대한 접속을 원할 경우, (그림 11)과 같이 변경이 가능하다. (그림 11)의 (1)에서 사용자가 임의로 지정된 Major 및 Minor 값을 변경하여 새로운 AP(SSID: PublicWiFi@skku.nrlab2)에 접속할 경우, 하단의 Major 및 Minor을 지정할 수 있다. 변경된 값을 설정하여 (그림 11)의 (2)번과 같이 'SET BEACON'을 누르면 사용자 디바이스는 iBeacon 디바이스와의 통신을 통해 Major 및 Minor 값을 변경한다. 변경된 값은 (그림 11)의 (3)번에서와 같이 iBeacon의 Major 및 Minor 값이 변경되었을 볼 수 있고, 이를 통해 AP가 PubliWiFi@skku.nrlab에서 PublicWiFi@skku.nrlab2로 변경된 것을 확인 할 수 있다.

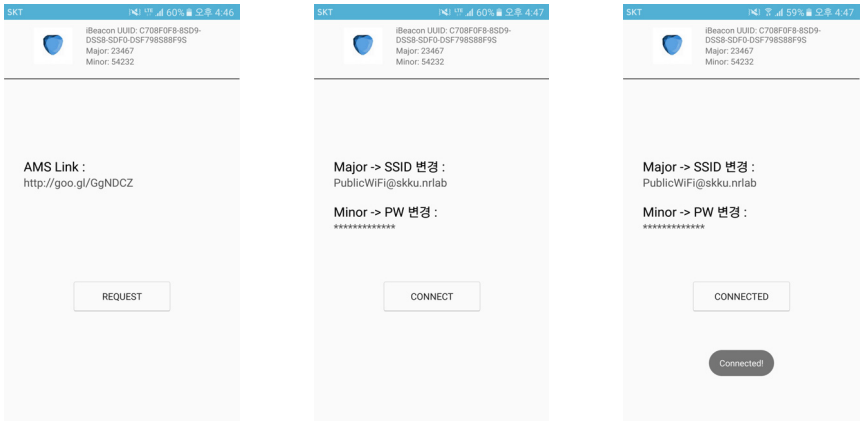
SSID와 PW를 App에서 미리 설정한 값을 통해 얻기보다는 서버를 통해 관리된 값을 받아올 수 있다. 이는 3.2에서와 같이 서버를 통해 AP의 등록된 정보를 받아오는 방식이다. (그림 12)의 (1)에서 iBeacon 메시지의 Major



(1) (2) (3)

(그림 11) App에서 Major 및 Minor 값 변경

(Figure 11) Changing Major and Minor values in App



(1) (2) (3)

(그림 12) AMS를 통한 AP 자동 접속

(Figure 12) Automatic AP access by AMS

및 Minor 값을 해석하여 하나의 링크(AMS 서버 url)로 변경할 수 있다. 이를 (그림 12)의 (2)와 같이 iBeacon 디바이스의 UUID를 AMS 서버로 보내어 iBeacon 디바이스를 통해 접속할 수 있는 AP의 정보(SSID 및 PW)를 AMS로부터 수신하여 수신된 값을 보여줄 수 있다. 이를 통해 사용자가 AP에 접속을 원하면 (그림 12)의 (3)과 같이 접속 할 수 있다.

5. 결 론

본 논문은 iBeacon을 이용하여 공공 무선랜 형식의 표준 기를 기반으로 AP에 자동적으로 접속하기 위한 방안을 제시하였다. 이를 위해 App내에서 AP 접속을 위한 방안뿐만 아니라, 외부 서버인 AMS를 통해 실시간으로 AP접속 정보를 제공할 수 있는 방안을 구현하였다. 보통의 AP 접속처럼 사용자의 추가적인 작업을 통해 접속이 이루어지는 것이 아니라 iBeacon을 수신할 수 있는 상태만 가능하다면 자동적으로 공공 무선랜에 접속 가능한 기술이다. 사용자 App으로 Android 기반의 스마트폰을 기반으로 구현되었고, 서버는 http통신을 통해 이루어졌다. 이를 통해 본 연구가 상품 판매를 촉진 위해 상점에서 배포하는 스

마트 디바이스용 App에 부가적인 기능으로 활용될 수 있을 것이다.

참고문헌(References)

[1] Digieco, “2015 first half year mobile trend”, 2015. http://www.digieco.co.kr/KTData/Report/FILE/PDF/2015%EB%85%84%20%EC%83%81%EB%B0%98%EA%B8%B0%20%EB%AA%A8%EB%B0%94%EC%9D%BC%20%ED%8A%B8%EB%A0%8C%EB%93%9C20150709143640546284 5.pdf?

[2] Kleiner Perkins Caufield & Byers, ″2015 Internet Trends Report″, 2015. http://www.kpcb.com/internet-trends

[3] MSIP and KISA, “2015 Survay on the Mobile Internet Usage Executive Summary”, 2014. http://isis.kisa.or.kr/board/?pageId=060300&bbsId=10&itemId=343&pageIndex=1

[4] RFC 4187, J. Arkko, H. Haverinen, “Extensible Authentication Protocol Method for 3rd Gerneration Authentication and Key Agrrement(EAP-AKA)”, January, 2006. https://tools.ietf.org/html/rfc4187

[5] Choi Byung-ik, Shin Jun-ho, ″A Study on the Public Wi-Fi Service Provision Model″, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.641-642, 2013.

[6] TTAK.KO-06.0253, ″WLAN Internet Service Provision Guideline for Public Sectors″, TTA Journal, Vol.134, pp.71-74, 2011.

[7] Andy Cavallini, ″iBeacons Bible 2.0″ https://meetingofideas.files.wordpress.com/2014/06/ibeacon-bible-2-0.pdf

[8] Markus Köhne, Jürgen Sieck, ″Location-based Services with iBeacon Technology″, Proceedings of International Conference on Artificial Intelligence, Modelling and Simulation, pp.315-321, 2014. http://dx.doi.org/10.1109/AIMS.2014.58

[9] Dominique Guinard, Vlad Trifa, Erik Wilde, ″A Resource Oriented Architecture for the Web of Things,″ Internet of Things(IOT), Tokyo, Nov, 2010. http://dx.doi.org/10.1109/IOT.2010.5678452

[10] Vlad Trifa and Dominique Guinard, ‘Towards the Web of Things, whitepaper 1.0″,: http://webofthings.org/wp-content/uploads/2009/05/wot-whitepaper.pdf

[11] RFC 7159, T. Bray, ″The Javascript Object Notation (JSON) Data interchange Format″, 2014. https://tools.ietf.org/html/rfc7159

[12] Google URL shortener, https://goo.gl/

[13] Starbucks mobile ap https://play.google.com/store/apps/details?id=com.starbucks.co

[14] Syrup mobile app, http://www.syrup.co.kr/index.do#about_syrup

◐ 저 자 소 개 ◑

남 춘 성(Choon-Sung Nam)

2005년 상명대학교 소프트웨어학과(이학사)
2007년 숭실대학교 대학원 컴퓨터학과(공학석사)
2011년 성균관대학교 대학원 전자전기컴퓨터학과(공학박사)
2014년 연세대학교 IT정책전략연구소 박사후연구원
2016년 성균관대학교 컨버전스연구소 선임연구원
관심분야 : VANET, IoT, UAV & Force Touch Interaction, tec
E-mail : namgun99@gmail.com

신 동 렬(Dong-Ryeol Shin)

1980년 성균관대학교 전자공학과(공학사)
1982년 KAIST 대학원 전기 및 전자공학과(공학석사)
1992년 Georgia Tech, 대학교 전기 및 전자공학과(공학박사)
1994년~현재 성균관대학교 정보통신공학과 교수 .
관심분야 : 유비쿼터스 컴퓨팅, 센서 네트워크 etc.
E-mail : drshin@skku.edu