비콘 서비스를 위한 보안 인증 방법

오정규*, 신지선**, 김형석***
*세종대학교 정보통신공학과
**세종대학교 정보보호학과 교수
***세종대학교 정보통신공학과 교수 (교신저자)
e-mail : hhh2123623@gmail.com

Authentication for Beacon Service

Jeong-Gyu Oh*, Hyung-Seok Kim**
*Dept. of Information and Communication Eng., Sejong University
**Dept. of Information and Security, Sejong University
*** Dept. of Information and Communication Eng., Sejong University

요 약

정보통신 기술의 발달로 사물인터넷에 대한 관심이 증가하였다. 사물인터넷의 한 요소인 무선 근거리 통신 기술에는 WiFi, 블루투스, ZigBee 등이 있다. 이러한 기술들 중 저전력 블루투스는 낮은 전력 소비와 범용성 덕분에 많은 각광을 받고 있다. BLE(Bluetooth LE)의 한 형태인 비콘은 더욱 저전력이며, 패킷을 전달하는 방식 또한 기존의 블루투스와 차이가 있다. 본 논문에서는 컨텐츠 보안이 필요한 비콘 서비스의 예시로 비콘을 통한 새로운 형태의 음악 음반을 제시하였다. 또한, 그 보안 특성에 맞춰 패킷 이중화, RSSI, Serial Number Binding 등의 기술들을 사용한 보안 방법을 설계 및 구현한 보안 사례에 대하여 서술한다.

1. 서론

최근 스마트폰, 태블릿 등의 스마트 디바이스가 매우 빠르게 보급됨에 따라 사물인터넷(IoT, Internet of Things)에 대한 관심이 증가하고 있다. 사물 인터넷은 사람과 사물 간의 통신을 넘어 사물들 간에 상호작용을 한다는 개념으로 확대되고 있다. 사물 인터넷에 대한 관심이 증가함에 따라 사물 간의 통신 기술 또한 화두가 되고있다. WiFI, NFC, Bluetooth, ZigBee 등의 다양한 무선 통신 기술들이 존재하는데, 그 중 Apple 社에서 개발한 Bluetooth LE(Bluetooth v4.0)의 한 프로토콜인 iBeacon 은 코인 셀 배터리 한 개로 약 1 년의 작동 시간을 가질 정도로 저전력이고, 소형으로 제작이 가능하다는 장점이 있다. 하지만 비콘은 고정된 패킷을 전송하기 때문에 보안에 취약할 수 있다. 본 논문에서는 사례를 통하여 보안을 적용한 새로운 형태의 비콘 서비스를 위한 인증 방법을 제안한다. 비콘 음반 플랫폼을 서비스의 한 예시로 제시한다. 정보통신 기술의 발달로 데이터에 대한 비용이 급격히 줄어 음악 감상은 대부분 스트리밍을 통해 듣는 시대가 되었다. 하지만 음반 앨범은 이러한 기술들의 발달을 쫓지 못하고 여전히 CD 라는 다소 도태된 저장장치에 저장되어 출시가 되고 있다. 스마트폰으로 모든 일을 처리할 수 있는 시대에 CD 플레이어를 통하여 음악을 듣는 사람은 매우 드물다. 이러한 음반 앨범이 판매되는 이유는 음악을 듣는 것이 아니라 팬들의 소장욕구에 의한 것이다. 사용자의 소장욕구를 더욱 충족시켜주고, 최신 기술 트렌드와도 부합하는 음반을 제작한 사례이다. 음반에 비콘의 장점들을 활용하여 새로운 형태의 음반을 제작하였다[1]. 음반은 사용함에 있어서 영구성이 있어야 하고, 저작권을 가지고 있어야 하기 때문에 불법 이용이 불가능해야한다. 비콘의 저전력이라는 특성은 음반의 영구성에는 부합되지만, 패킷을 공개적으로 브로드캐스트한다는 점 때문에 보안에 취약할 수 있다. 사용자는 비콘 음반을 스마트폰으로 스캔하여 서버로 보내고, 서버에서 음반을 인증받고, 등록함으로써 그 음반의 권한을 부여받는 과정을 거친다. 이 때, 안전한 인증 및 등록과정 및 다른 비콘 음반 패킷을 유추할 수 없게 만들어야 한다. 가령, 유료 소프트웨어 패키지를 구매할 때 사용자는 CD 와 함께 동봉된 시리얼 번호를 입력하여 안전하게 인증받는 과정을 거친다. 또한, 이러한 시리얼 번호를 통해 같은 소프트웨어의 다른 시리얼번호가 유추되는 상황은 없어야 되는 상황과 같다. 이러한 상황에서 안전한 인증 및 보안을 위해 아이비콘에 패킷 이중화, RSSI, Serial Number Binding 을 적용하는 방법을 제안한다. 제 2 장에서는 인증 보안에 관련된 연구에 관하여 설명한다. 이러한 비콘 서비스에 대한 인증 방법을 통해 사물인터넷 분야에서 다양한 기회를 제공하는 것을 목표로 한다.

본 연구는 NRF-2016R1A2B4008457 의 지원을 받아 수행되었습니다.

2. BLE 비콘

3.1 IoT 분야에서 활용되고 있는 비콘

비콘은 블루투스 Low Engergy(BLE) 기반의 프로토콜이다. BLE 는 iOS, Android 등의 대부분 스마트폰에 내장되어 있고, 다양한 블루투스를 탑재한 제품들도 출시되고 있다. 비콘은 UUID (Universally unique identifier)와 Major, Minor 로 구성되어 있고, 이 값들을 일정한 주기에 따라 브로드캐스트한다. 기존의 블루투스와는 다르게 비연결 기반으로, 단방향성 통신 프로토콜이다. 비콘은 NFC 와 비교되며, 통신 거리가 길며, 다양한 단말들과 동시에 통신할 수 있다는 장점을 갖는다.

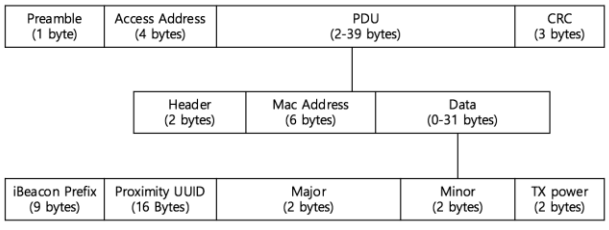
구 분	비 콘	NFC
기반 기술	Bluetooth LE	RFID
범 위	50m	5cm
특 징	P2P(Multi Point)	P2P
지원 OS	Android, iOS	Android
주파수	2.4-2.5GHz	13.56MHz
통신방향	단방향	양방향

(표 1) BLE 비콘과 NFC 비교

이러한 비콘의 특성 때문에 사물 인터넷의 여러 분야에서 활용이 되고 있다. 전자출결관리 시스템 U-Check 는 수업이 있는 강의실에서 비콘 패킷을 전송하고, 사용자의 스마트폰은 비콘 패킷을 수신한다. 스마트폰은 비콘 패킷을 통해 사용자가 출석을 했다는 요청을 보내는 방식이다. 또 다른 활용은 얍 社의 비콘이다. 얍 컴퍼니의 비콘은 하이브리드 비콘이라고 불린다. 하이브리드 비콘은 고주파 신호와 비콘을 결합한 형태이다. 하이브리드 비콘은 스타벅스 매장에서 '프리오더'라는 이름으로 서비스되고 있다. 매장 내에서 줄을 서지 않고 앱을 통해 주문하는 시스템이다. 이처럼 비콘은 사물 인터넷에서 다양한 서비스 형태로 사용이 되고 있다.

3.2 RSSI(Received Signal Strength Indicator)

BLE 는 총 47Bytes 의 Advertising Data 를 사용한다. Advertising Data 의 구조는 다음과 같다. 비콘은 BLE 의 PDU 중 31Bytes 의 Data 부분에 정의된다. 9Bytes 의 iBeacon Prefix 에는 Header, Flag, Company ID, iBeacon Type, iBeacon Length 가 정의된다[2].



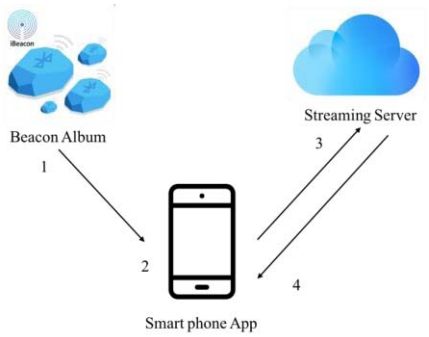
(그림 1) BLE 비콘 패킷 구조

비콘의 Tx Power 필드는 비콘의 수신 신호 세기를 의미한다. RSSI 라고도 불리며, dBm 의 단위를 사용한다. RSSI 는 거리의 제곱에 반비례하기 때문에 RSSI 를 통해 비콘과 비콘 패킷을 전달 받는 스마트폰과의 거리 예측이 가능하다. 하지만 현실에서는 장애물, 백색잡음 등의 여러가지 요소에 영향을 받을 수 밖에 없다. 이러한 비콘의 환경에서 오차 범위를 줄이려는 다양한 연구들이 진행되고 있다[3].

비콘이 적용된 분야의 서비스들은 일반적으로 위치 기반의 O2O 서비스 (Online to Offline Service) 이다. O2O 서비스는 보통 위의 예처럼 일반 대중들에게 공개적이다. 즉, 동일한 패킷을 주기적으로 송신하고, 그 위치에 있는 사용자의 스마트폰이 수신하여 서비스를 이용한다. 비콘의 이러한 특성은 사용자에게 노출이 빈번하게 일어나고, 그 데이터들이 노출이 되어도 보안상 문제가 되지않는 서비스에 적합하다. 비콘에 보안 문제만 해결되면, 이전의 서비스들보다 더욱 다양한 서비스에 적용이 가능하다. 비콘에 보안이 적용되어 특정 사용자만 사용할 수 있거나, 복제가 불가능하다면 비콘 모듈을 통한 새로운 제품 생산이 가능하다. 본 논문은 비콘에 보안을 필요료 하는 한 제품의 예시를 설명하고, iBeacon 규격 비콘에 보안을 적용하는 방법에 대해서 설명하고, 실제 제품으로 제작하였을 때 보안 및 성능에서 문제가 없다는 것을 실험을 통하여 검증하는 것을 목표로 한다.

3. 제안하는 방법

본 논문에서 제안하는 비콘 음반 인증 및 등록 방법은 다음과 같다. 비콘 음반은 iBeacon 규격에 맞춰 UUID, Major, Minor 값을 2 번에 나눠 이중화 하여 일정 주기 동안 반복하여 값을 브로드캐스팅한다. 사용자는 모바일 어플리케이션에 로그인하고 비콘 음반을 스캐닝 한다. 어플리케이션에서 스캔된 아이비콘들의 UUID, Major, Minor, RSSI 값과 로그인된 사용자 정보를 서버에 보내 비콘음반 인증을 요청한다. 서버는 UUID, Major, Minor 값과 로그인된 사용자 정보를 DB 에 등록된 비콘음반 정보들과 대조하여 인증 절차를 거치고, 미등록 비콘음반이며, RSSI 값이 일정 값 이내이면 로그인된 사용자에게 등록 권한을 부여하고, 등록하면 음반 컨텐츠 접속 권한을 부여한다. 기등록 비콘음반이며, 로그인된 사용자 정보도 바르게 매칭되어 있으면 음반 컨텐츠 접속 권한을 부여한다.



(그림 2) 비콘 음반 인증 절차

4.1 시스템 구성

하나의 앨범은 고유한 시리얼 넘버를 갖는다. 시리얼 번호는 각 비콘과 서버에 약속이 되어있다. 각 비콘은 하나의 앨범으로써 각각의 앨범들이 모두 고유한 값들을 갖는다. 시리얼 번호의 구성은 다음과 같다.

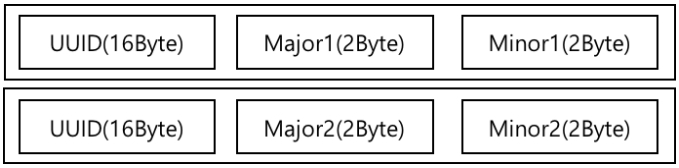


Figure 2. 비콘 앨범의 시리얼 번호 구성

16 바이트의 UUID, 각 4 바이트인 2 쌍의 Major Minor 로 총 24 바이트가 시리얼 넘버가 된다. 각 앨범 서로 다른 값들을 가진다. 시리얼 넘버의 예는 다음과 같다.

UUID : E20A39F4-73F5-4BC4-A12F-17D1Ad07A968

Major1 : 2735, Minor1 : 4832

Major2 : 4632, Minor2 : 8623

비콘은 본래 고정된 UUID 와 Major, Minor 만을 브로드캐스팅하기 때문에 하나의 고정된 값을 음반으로 사용을 하게 되면 한 가지 문제가 생길 수 있다. 음반이 아닌 다른 용도로 사용되는 비콘과의 충돌의 염려가 생긴다. 비록 비콘의 총 패킷이 20 바이트로 매우 커 중복될 가능성이 매우 낮지만, 소유권과 고유성이 보장이 되어야하기 때문에 두 개의 패킷을 사용함으로써 이를 해결하였다.

사용자는 음반을 처음 구매하였을 때 스마트폰을 통하여 음반을 등록한다.비콘은 신호를 브로드캐스팅하기 때문에 사용자가 등록을 시도하려고 비콘 음반을 켰을 때 비콘 패킷 스나이핑을 통한 타인의 음반 등록 위험에 노출될 수 있다.이러한 점은 비콘과 스마트폰의 거리를 통해 해결하였다. 비콘의 신호 세기를 의미하는 RSSI 를 통하여 Proximity 를 측정할 수 있다. 애플은 비콘의 Ranging 모드에서 Proximity 를 다음과 같이 구분을 하여 사용할 것을 권장하고 있다[3]. 음반을 등록할 때 등록되지 않은 비콘이 스마트폰과의 거리가 일정 시간동안 Immediate 를 유지할 때 등록할 수 있도록 제한을 두었다.

TABLE I. 비콘 PROXIMITY 에 대한 표현

구 분	표 현
0.5m 이내	Immediate
0.5m ~ 3m	Near
3m ~	Far

4.2 인증 절차

4.2.1 Serial Number Binding 을 통한 음반 등록

비콘 음반을 처음 구매했을 때 사용자는 스마트폰을 통해 비콘을 스캔한다. 스마트폰은 각 비콘의 Proximity 를 측정하여 약 5sec 간 Immediate 를 유지할 때 서버로 전송한다. 서버로 전송할 때 데이터는 다음과 같다.

{

User_id : String(16Bytes),

Mac Address : String(6Bytes),

UUID : String(16Bytes),

Major : String(2Bytes),

Minor : String(2Bytes)

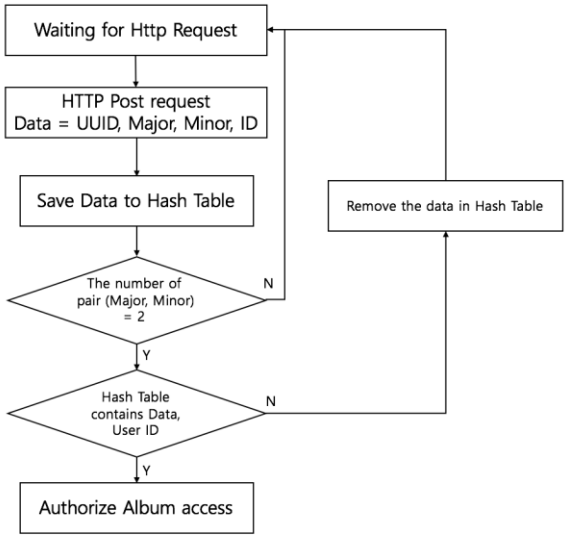
}

스마트폰은 Proximity 의 조건을 만족한 비콘의 값들을 위와 같이 Json Object 를 생성하여 서버에 전달한다.각 비콘 음반은 고유한 UUID 를 가지고 있으며,이러한 UUID 는 Random Seed 에 의해 생성된다. UUID 는 음반 자체의 고유한 ID 를 의미한다.서버에는 DB 에 각 비콘 음반의 고유한 UUID 를 저장하고 있다.DB 는 KEY-VALUE 방식의 NoSql 인 Redis 를 사용하여 UUID 는 Hash table 의 KEY 와 같은 역할을 한다. VALUE 로는 사용자의 id, 해시 함수, 해시 함수를 통해 만들어진 Major, Minor 등의 정보가 Json 타입으로 저장된다.사용자의 id 는 사용자가 자신이 구매한 비콘을 등록 할 때 Binding 된다. 이렇게 Serial Number (UUID)를 사용자의 id 와 binding 함으로써 복제된 비콘에게 음반 정보에 대한 권한을 막을 수 있다.

4.2.2 음반 권한 인증

서버에서 음반에 대한 권한을 인증받는 흐름은 다음과 같다. UUID 와 Major, Major 이 담긴 HTTP 요청이 오면, Hash table 에 저장을 한다. 패킷 이중화에 의한 두 번의 요청이 모두 오면, 서로 다른 두 개의 Major, Minor 가 테이블에 저장된다. 테이블에서 비콘의 UUID 로부터 User ID 와 Binding 여부를 확인하고, 두 개의 Major 와 Minor 또한 확인한다. 이러한 확인이 완료되면 서버는 음반에 대한 권한을 사용자에게 부여한다. 서버에서

사용자에게 음반에 대한 권한을 부여하는 flow 는 다음과 같다.

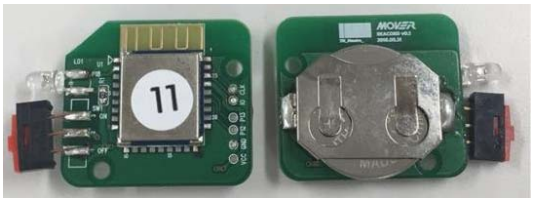


(그림 3) 앨범 액세스 권한 흐름도

4.3 개발 환경

4.3.1 비콘 음반

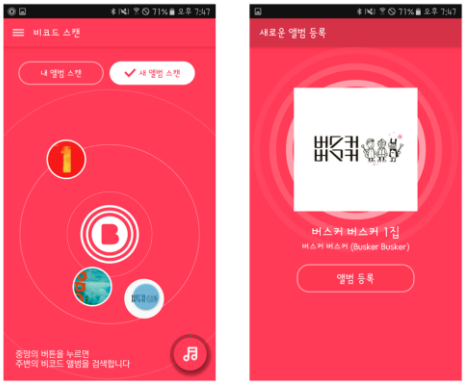
Beacon 펌웨어 개발은 mbed Nordic nRF51-dk 보드에서 개발하였고, 비콘 음반에는 Norfic nRF51822 모듈을 사용하였다.



(그림 4) 비콘 음반 인증 절차

4.3.2 어플리케이션

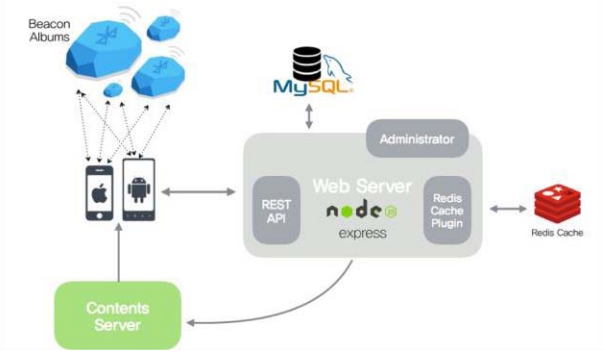
스마트폰 어플리케이션 개발 환경은 안드로이드 스마트폰을 사용하였다.테스트 기기는 Nexus5 (Andoroid v6.0.1), Galaxy S6(Android v6.0.1), Galaxy S5(Android v5.1)이다.



(그림 5) 비콘 음반 스캔 및 등록

4.3.3 서버

서버는 Ubuntu 14.04.3 LTS 버전 에서 개발하였다. 개발 환경으로는 Node.js(v6.2.1), mysql, redis, Express, Nginx 등을 사용하였다.



(그림 6) 비콘 음반 서버 구성

4. 결론

본 논문에서는 비콘을 서비스로써 사용할 때 인증에 대한 절차에 대하여 서술하였다. 그 예시로 음반의 새로운 포맷으로 활용되는 상황을 설명하고, 비콘에 대한 인증 방법을 제안하였다. 제안하는 과정에서 비콘의 기술적 스펙을 서술하고, 비콘의 기술적 특징들을 음반이라는 특수한 경우에 적용하기 위한 당위성을 부여하였다. 본 논문에서의 연구는 비콘 음반을 실제 환경의 서비스에 적용과 동시에 지속적 추가 연구 개발의 토대가 될 것이다.

참고문헌

[1] “Beacons: The Technical Overview”, Mubaloo
[2] http://beacord.xyz Beacord, Mover
[3] https://developer.bluetooth.org
[4] https://developer.apple.com/iBeacon/
[5] 비콘을 이용한 자동 출결 시스템 서비스, 오주현, 아주대학교 정보컴퓨터공학과