BLE デバイスからのプライバシー問題に関する安全性の評価

原田 玲央†
明治大学総合数理学部先端メディアサイエンス学科†

1. はじめに

私たちは常にスマートホンをはじめとするデバイスを持ち歩き，インターネットにいつでも接続できる環境下にある．さらに Bluetooth Low Energy(以後，BLE と呼ぶ)が普及したことにより容易に様々な情報の交換がされるようになった．今後，イヤホンやスマートウォッチなどユーザー一人に対して身につける BLE デバイス数が増加することが想定される．

Bluetooth デバイスにはデバイス固有のアドレス(MAC アドレス)が振られているので，プライバシーに関するリスクも考えなければならない．高木は，山手線の車内で観測できる Bluetooth デバイスの MAC アドレスを収集することによって,得られたデータから乗降パターンが追跡されてしまうリスクを提示している[1]．このように，デバイス固有の情報をスキャンすることで Bluetooth デバイスを利用しているユーザーの行動パターンというプライバシー関わる情報が第三者に漏洩してしまう恐れがある．

そこで，近年普及してきている BLE に注目し，通信から Bluetooth デバイスの情報がどのくらい取得できるか検証し，Bluetooth デバイスによるプライバシー問題に関する安全性について明らかにすることを本研究の目標とする．

2. Bluetooth 通信観測実験

2.1 概要

本実験は，PC やスマートホンなどのデバイスの BLE 通信をスプーフィングすることで，デバイスの情報を取得できるか検証する．

図 1 に本実験の構成を示す．アドバタイジングパケットをブロードキャストするビーコン A を用意し，それらを受け取ったデバイスが返送する ADV_SCAN_REQ パケットを CC2540 USB 評価モジュール・キット[2]で拾うことにより，周囲にある全ての Bluetooth デバイスの MAC アドレスを収集する．CC2540 で収集したデータは専用のパケットスニッファ形式である psd ファイル(packet sniffer data)に保存される．観測データをあらかじめ調べておいた Bluetooth デバイスの MAC アドレスのリスト(以後，評価用データと示す)と照合し，取得できるデバイス数を評価する．

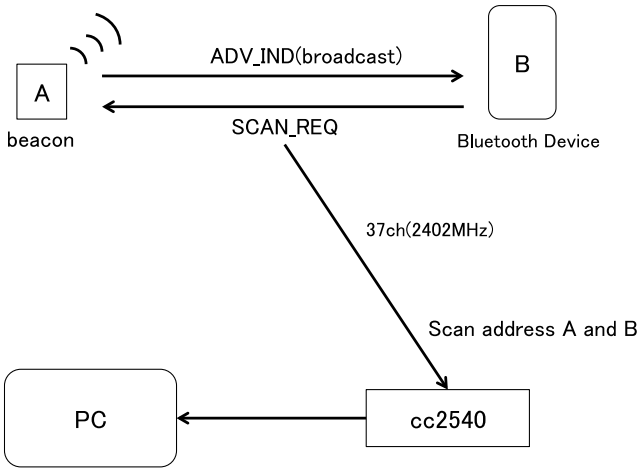

図 1:デバイス情報の収集方法

2.2 変換プログラム psd2csv

CC2540 を用いて取得できたパケットは独自フォーマットである psd 形式で保存される．本データを R などのツールを用いて解析できるように，csv として出力する psd2csv を processing で実装した．psd2csv は csv 形式の評価用データと BLE パケットが含まれる psd ファイルを入力として，検出された ADV_SCAN_REQ パケットと検知されたデバイスを集計する csv ファイルを出力する．

2.3 データ形式

表 1 に CC2540 で収集した情報，2.1 節で示した評価用データ,psd2csv で出力する情報を示す．psd2csv は CC2540 が取得した情報から本実験で扱う情報のみを抽出し，評価用データと結びつけて出力する．

表 1:各データファイルの取得情報

取得情報	CC2540	評価データ	psd2csv
TimeStamp	○	×	○
PDU Type	○	×	○
AdvA	○	×	○
ScanA	○	○	○
RSSI	○	×	○
AccessAddress	○	×	×
PDU Header	○	×	×
Channel	○	×	×
CRC	○	×	×
FCS	○	×	×
DeviceName	×	○	○
User	×	○	○

Evaluation of the safety of privacy issues from the BLE devices
† REO HARADA
Department of Frontier Media Science, Faculty of Interdisciplinary Mathematic Science, Meiji University.

3. 評価

3.1 取得できたデバイス数

2015 年 11 月 17 日に実験室にて研究室の学生が持つデバイス 19 台を対象に実験を行った．観測地点の周囲（半径 3m 以内）に Bluetooth デバイスをランダムに配置する．検証時間を 100s とし，BLE のアドバタイジングチャンネルである 37ch(2402MHz)におけるパケットを収集した．デバイスは Bluetooth を ON 状態とし，観測中の位置は動かさない．

あらかじめ調査した対象デバイスの MAC アドレスに対して，BLE パケットから得られた Scan Address が一致したデバイスの数を表 2 の B に示す．BLE パケットから得られたデバイスは 4 台(4/19=21%)である．デバイスの種類で見ると，MacBook と Mac mini が検出されたのに対して Android 端末や iPhone といったスマートホンやレガシー携帯電話は検出されなかった．

表 2:評価用データ及び検出数

デバイスの種類	デバイス数(A)	検出数(B)
Android	4	0
iPhone (iOS)	6	0
Mac Book (OS X)	4	3
Mac mini (OS X)	1	1
LaptopPC(Windows)	2	0
Mobile phone	1	0
Fit-bit	1	0

3.2 検出時間と RSSI

検出されたデバイスの時間変動に対する BLE 通信の受信信号強度 RSSI(Received Signal Strength Indication)の安定性を明らかにするため，3.1 節で psd2csv により取得したデータを R で解析した．図 2 に，検出されたパケットの RSSI の時間推移を示す．評価用データとアドレスが一致したデバイスのパケットを•で示し，それ以外のアドレスのパケットを×で示す．また，表 3 の C に RSSI の標準偏差，D に変動係数を示し，観測デバイス a, b, c, d とする． デバイス d は，abc に比べて RSSI のばらつきが大きく，周囲の人の動きなどの外的要因があると推測される． しかし， d を除いて固定されたデバイスの RSSI の標準偏差は 2.44 から 3.40 であり安定していると考えられるが，高精度な位置関係を導出するには十分な安定性とはいえない．また，評価用データとアドレスが一致しない unknown アドレスが検出された．Unknown アドレスは-90 dBm 付近に分布しており，実験室外のデバイスが検出されたと推測される．

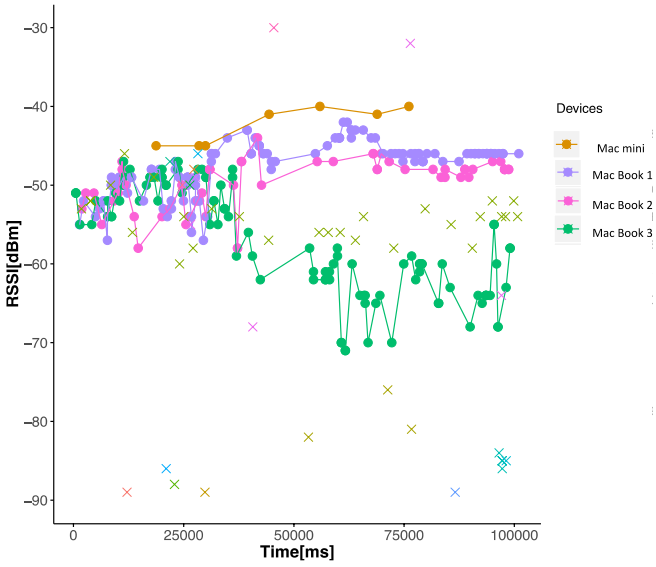

図 2:検出されたパケットの RSSI

表 3:RSSI のばらつき

デバイス	標準偏差(C)	変動係数(D)
Mac mini (a)	2.44	5.8%
Mac Book 1 (b)	3.40	7.1%
Mac Book 2 (c)	3.22	6.5%
Mac Book 3 (d)	6.79	11.9%

4. おわりに

BLE の ADV_SCAN_REQ パケットから周辺デバイス情報の取得が可能であることを検証した．2 節での手法では一部のデバイスしか読み取ることができなかったが，Bluetooth デバイスからユーザーの行動パターンを読み取る脅威が存在するのではないかと考える．

一方，本実験において検出されなかったデバイスが多数みられた．本実験は 3 つのアドバタイジングチャンネルのうち 1 つの通信経路における調査結果であり，本実験で検出できなかったデバイスが他のチャンネルに流れている可能性があげられる．もしくは，検出が容易にできないように BLE 規格が設計されているのではないかと考える．

参考文献

[1] 高木浩光, Bluetooth で山手線の乗降パターンを追跡してみた, (http://takagi-hiromitsu.jp/diary/20090301.html, 2015 年 6 月参照).

[2] TEXAS INSTRUMENTS,CC2540 USB 評価モジュール・キット (http://www.tij.co.jp/tool/jp/cc2540emk-usb, 2015 年 5 月参照).

[3] 鄭立, Bluetooth 入門, 秀和システム(2014).

[4] 折尾彰吾, 上田浩, 上原哲太郎, 津田侑, ワイヤレスデバイスのもたらすロケーションプライバシー問題に関する一察, コンピュータセキュリティシンポジウム 2012, pp. 262-269, (2012).