Lab # 2. BLE

Adan Abu Naaj — adann@mit.edu
Artem Laptiev — laptiev@mit.edu

6.1820

March 11, 2025

1 BLE Discovery

A central device (our phones in this lab) uses Bluetooth Low Energy (BLE) scanning to detect nearby peripherals. First, the peripheral (in this lab, the anthill) broadcasts data packets called advertisements. These packets include the peripheral's unique identifier, services, characteristics, and, if available, the device name. After advertising, the central device begins scanning using the CoreBluetooth framework. The central listens for advertisement packets, and once an advertisement is received, the phone's BLE stack triggers a callback (in our code: didDiscoverPeripheral) and provides details of the discovered peripheral such as its identifier, name, and signal strength. Then, after discovering a peripheral, the phone establishes a connection. In our lab, the phone connects to the first peripheral found in range and remains connected until the peripheral is no longer in range (or its Bluetooth services are turned off). In other networks, a more advanced decision-making process for peripheral connection could be used. Once connected to a peripheral, we can access its services and characteristics to retrieve data. In this lab, we obtain sensor readings from the anthill sensor, which include humidity and temperature.

The figure below depicts the advertisement between central and peripheral (Apple Inc. Core Bluetooth Overview. Figure 1-2)

Figure 1: Advertising and discovery.

2 A peripheral, a service, a characteristic

In BLE, these terms define a hierarchy that organizes how data is structured and accessed: Peripheral: A physical BLE device that contains data and functionality and advertises its presence to a central device. In this lab, the anthill sensor is the peripheral. Service: A grouping of data and behaviors offered by a peripheral. Services provide a way to organize features; for example, in our lab, a service includes both humidity and temperature readings. Characteristic: The smallest data unit offered by a peripheral. It contains a specific piece of data and properties that describe how that data can be accessed or modified. In our lab, the data are the temperature and humidity values, and the property is "read"—other properties might allow for writing or notifications. The relationship between these components is that a peripheral can host one or more services, and each service includes characteristics, which are the data points that the central can, for example, read from or write to.

The figure below depicts the hierarchical relationship between them (Apple Inc. Core Bluetooth Overview. Figure 1-5. Figure 1-3).

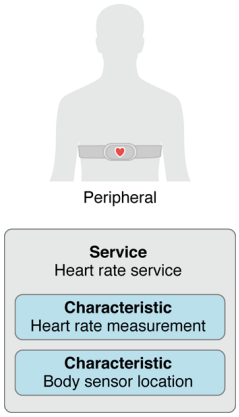

Figure 2: A remote peripheral's tree of services and characteristics.

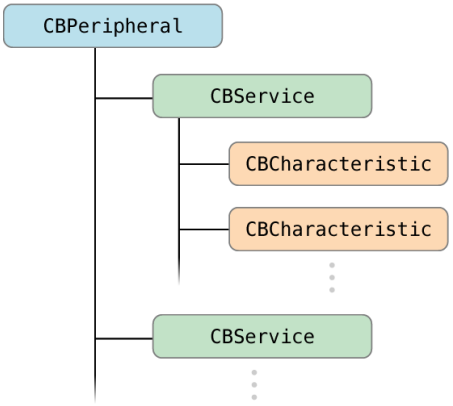

Figure 3: A peripheral's service and characteristics.

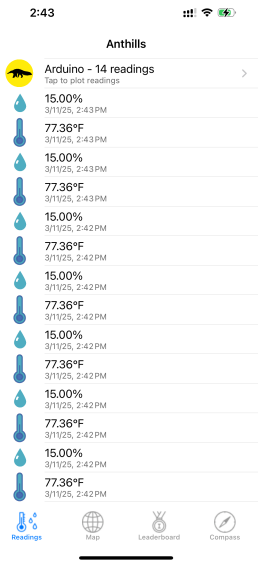

Figure 4: Anthill discovered and transmitting data to client device.

3 Time Spent

Time spent:

- Section 1: = 2 hour
- Section 2: = 1 hour
- Report: = 1 hour