
BLE 基础教程

——疯壳·开发板系列

Wolverine-Team

2015/3/13

目录

术语和定义.....	4
一、 BLE 简介.....	4
1.1 单模设备.....	4
1.2 双模设备.....	4
二、 BLE 协议栈介绍.....	5
2.1 BLE 协议栈的结构.....	5
2.2 协议栈中的分层.....	5
2.2.1 PHY 层.....	5
2.2.2 LL 层.....	5
2.2.3 L2CAP 层.....	5
2.2.4 SMP 层.....	5
2.2.5 ATT 层.....	6
2.2.6 GATT 层.....	6
2.2.7 GAP 层.....	6
2.3 设备状态.....	6
三、 BLE 相关参数.....	6
3.1 服务与特征值.....	6
3.2 特征值的权限.....	6
3.3 通信方式.....	6
3.4 广播.....	7

官网地址: <http://www.fengke.club>
购买链接: <http://shop115904315.taobao.com/>
官方 QQ 群: 193836402

术语和定义

BLE	低功耗蓝牙 (Bluetooth Low Energy)
SDK	软件开发工具包 (Software Development Kit)
UUID	通用唯一标识符 (Universally Unique Identifier)
APP	手机应用软件 (Application)
MAC	媒体访问控制 (Media Access Control)
PHY	物理层 (Physical Layer)
LL	链路层 (Link Layer)
L2CAP	逻辑链路控制与适配协议 (Logical Link Control and Adaptation Protocol)
SMP	安全管理协议 (Security Management Protocol)
ATT	属性协议 (Attribute Protocol)
GATT	通用属性配置 (Generic Attribute Profile)
GAP	通用接口配置 (Generic Access Profile)

一、BLE 简介

BLE 为低功耗蓝牙技术，是低成本、短距离、可互操作的鲁棒性无线技术，工作在免许可的 2.4GHz ISM 射频频段。BLE 有三大特性，分别为最大化的待机时间、快速连接和低峰值的发送/接收功耗。主要进行小数据包传输，低延迟，低功耗，应用于手机、个人电脑以及可穿戴设备等。不适合蓝牙耳机等高速率设备。

1.1 单模设备

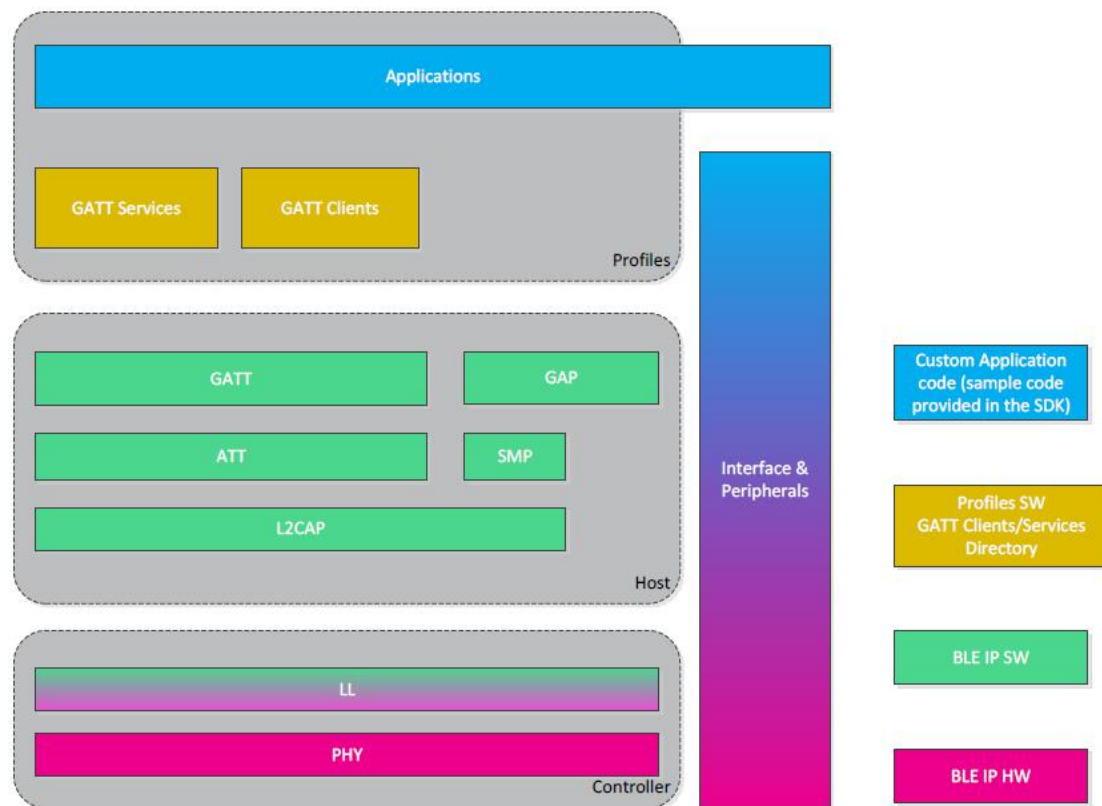
单模设备是指只支持 BasicRate(BR)或者 Bluetooth Low Energy(BLE)中的一种，本教程中是指支持 BLE 的设备。主要特点为低功耗和低速率。不兼容传统蓝牙，可兼容双模设备。

1.2 双模设备

双模设备是指同时支持 BR 与 BLE 的设备，双模设备为蓝牙 4.0 的主题，要有稳定的电源供电，比如手机、电脑等。Android 4.3 版本的系统才支持 BLE。iPhone4S 及以后的苹果手机均支持蓝牙 4.0。双模设备兼容 BLE 以及传统蓝牙。

二、BLE 协议栈介绍

2.1 BLE 协议栈的结构



- (1) 协议栈有两部分组成：Controller 和 Host；
- (2) Profiles 和 Applications 是基于 GAP 和 GATT 之上的；
- (3) 在单芯片工作模式中，Profiles、Host、Controller 三者都工作在 DA14580 芯片中。

2.2 协议栈中的分层

2.2.1 PHY 层

RF（天线）规格特性为：运行在 2.4GHz ISM band；GFSK（高斯频移键控）调制；40 频道 2MHz 的通道间隙（3 个固定的广播通道和 37 个自适应自动调频数据通道）。

2.2.2 LL 层

RF 控制层，控制芯片工作在 standby（准备）、advertising（广播）、scanning（监听/扫描）、initiating（发起连接）、connected（已连接）这 5 种状态中的一种。5 种状态的切换描述为：advertising（广播）不需要连接就可以发送数据（告诉所有人，我来了），scanning（监听/扫描）来自广播的数据，initiator（发起人）将携带 connection request（连接请求）来响应广播者，如果 advertiser（广播者）同意该请求，那么广播者和发起者都会进入已连接状态，发起连接的设备变为 master（主机），接收连接请求的设备变为 slave（从机）。

2.2.3 L2CAP 层

将数据打包，可以让设备点对点的通信。

2.2.4 SMP 层

安全管理服务层，提供配对和密钥的分发，实现安全连接和数据交换。

2.2.5 ATT 层

允许设备向另外一个设备展示一块特定的数据，称之为“属性”，在 ATT 环境中，展示“属性”的设备称为服务器，与之配对的设备称为客户端。链路层状态（主机和从机）与设备的 ATT 角色是相互独立的，也就是说，主机设备可以是 ATT 服务器，也可以是 ATT 客户端。从机也一样。

2.2.6 GATT 层

从名字就能看出，GATT 是在 ATT 上面的一层结构，定义了使用 ATT 的服务框架，GATT 规定了配置文件（profile）的结构。在 BLE 中，所有被 profile 或者服务用到的数据块都称为“特性”（characteristic）。两个建立连接的设备之间的所有数据通信都是通过 GATT 子程序处理，应用程序和 profile 直接使用 GATT 层。

2.2.7 GAP 层

General Access Profile 为基本访问配置，这个配置是其它配置的基础。它定义了 Bluetooth 设备间建立基带链路的通用方法

2.3 设备状态

BLE 设备有 6 种状态：

待机状态（Standby）：设备没有传输和发送数据，并且没有连接到任何设备。

广播状态（Advertiser）：周期性广播状态。

扫描状态（Scanner）：主动寻找正在广播的设备。

发起连接状态（Initiator）：主动向某个设备发起连接。

主设备（Master）：作为主设备连接到其他设备。

从设备（Slave）：作为从设备连接到其他设备。

三、BLE 相关参数

3.1 服务与特征值

为了实现用户的应用，Profile 通常有一个或者多个服务（Service）组成，每个服务对应特定的功能，比如体温服务、心率服务等。一个服务包含一个或多个特征值（characteristic value），比如心率服务中就会有一个心率特征值。每个特征值必须占用一个特征申明结构，其中包括它的其它特性，它是服务端和客户端共享的读写空间，设备之间的数据信息交换就是通过特征值。

UUID 是代表服务与特征值的通用唯一标识。有 128 位与 32 位两种形式。有一些服务已经配分配为固定的 UUID，所以用户自定义的服务与特征值不能使用这些 UUID。

3.2 特征值的权限

Permissions（权限）定义了特征值的访问权限，比如规定某个特征值只能被读，或者可读可写等。

3.3 通信方式

已连接设备之间的通信方式：

Read：使用指定的 handle 读特征值；

Write：使用指定的 handle 写特征值；

Indication：某个特征值发送到客户端，需要确认；

Notification：某个特征值发送到客户端，不需要确认，设备向手机 APP 发送数据的方法。

3.4 广播

广播包的发送是单向的，不需要任何连接。设备发送广播包进入广播状态。

广播包可以包含特定的数据定义，最大 31 个字节。

广播包可以直接指定特定的设备，也可以不指定。

广播包中可以声明是可被连接的设备，或者是不可连接的设备

广播间隔是指两次广播时间之间的最小间隔（0.625ms 的倍数+随机延时），其中随机延时为 0~10ms，为了避免多个设备之间的数据碰撞。

DA14580 的 BLE 协议栈只在 37 通道中广播。