青风带你玩蓝牙 nRF51822 系列教程

----------作者：青风

出品论坛：　www.qfv8.com　青风电子社区

作者： 青风
出品论坛: www.qfv8.com
淘宝店：http://qfv5.taobao.com
QQ 技术群：346518370
硬件平台：青云 QY-nRF51822 开发板

2.11 NRF51822 蓝牙数据传输分析

在使用 nrf51822 开发 BLE 应用中，有必要结合 nRF51822 的例程向工程师介绍 BLE 的广播和建立连接时通信数据包的相关内容

1：nRF51822 蓝牙通信包解析：

使用 Packet Sniffer 软件，配合青风的 usb dongle 抓包器进行抓包，首先我们分析一下 BLE 例程下的广播包的构成，使得大家能够直观的认清蓝牙广播包的构成，同时对蓝牙的 GAP 有一个深入的认识。

首先大家需要下载任何一个 BLE 蓝牙应用程序到我们的蓝牙开发板中，下列开发板都可以：

1.硬件开发板： (1)：青云 NRF51822 开发板

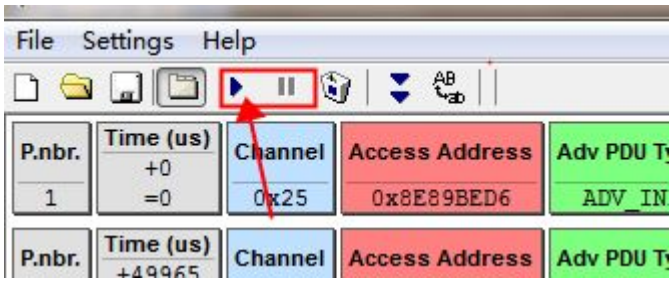
(2)：MINI 青云 NRF51822 开发板（发布）

(3)：豪华青云 NRF51822 开发板（发布）

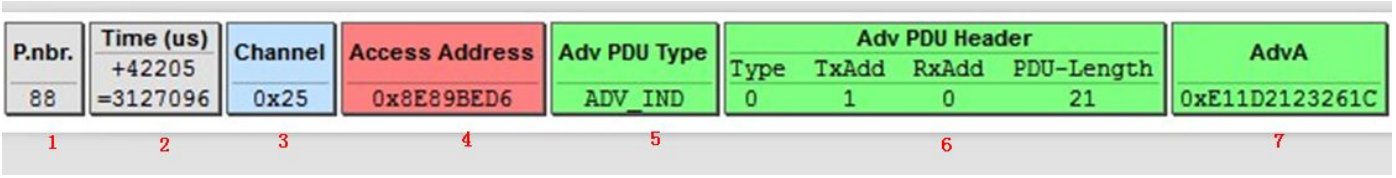
2.软件：Packet Sniffer，TI 官方开发的蓝牙 4.0 抓包软件，非常方便抓包，值得推荐：

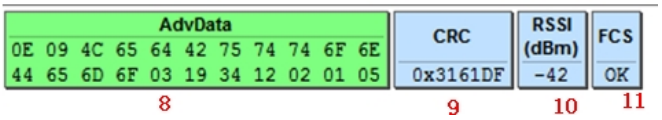
1.1 广播包抓取：

打开软件点击下图三角号后，就可以开始抓包：



抓到的包显示如下：





我们把广播包按照不同组成标记为 1 到 11 个部分，如上图所示。下面来一一分析：

第 1 部分：P.nbr.指的是 Packet Sniffer 抓的包的序列个数，这个依次计数，从 1 开始，依次计数。

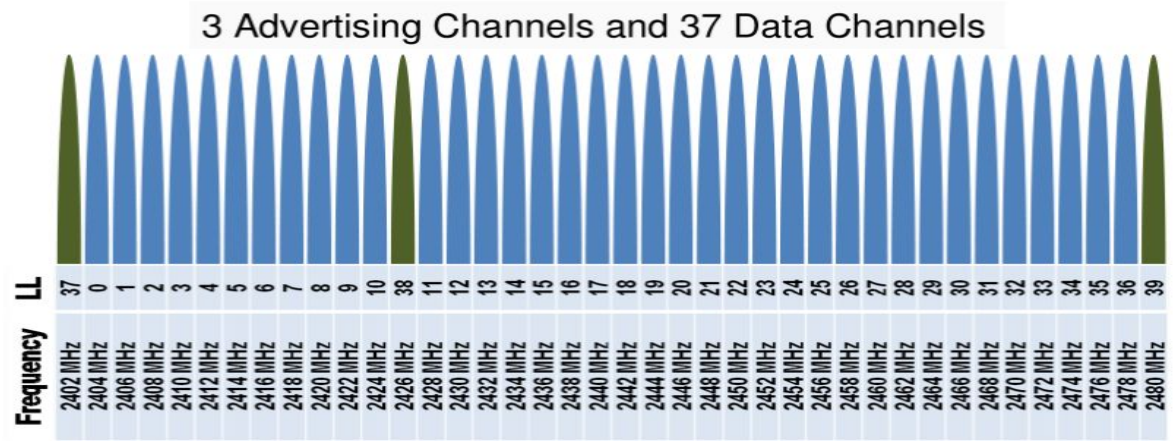
第 2 部分：Time(us)指的是抓取包的时间延迟。

第 3 部分：广播包表示的是广播信道，数据包表示的是数据信道。

数据链路层的 2 种信道：

1)广播信道：提供给还没有建立连接的蓝牙设备提供发射广播、扫描、建立连接的信道。 BLE 有 3 个广播信道:37、 38、 39,在每一个广播事件发生时， advertiser 分别在这 3 个信道上各发送一次广播信号。传统蓝牙的广播信道有 16-32 个，而 BLE 只有 3 个，这就是为什么 BLE 的广播时间比较短的原因。图中 0x25 为 37 信道。

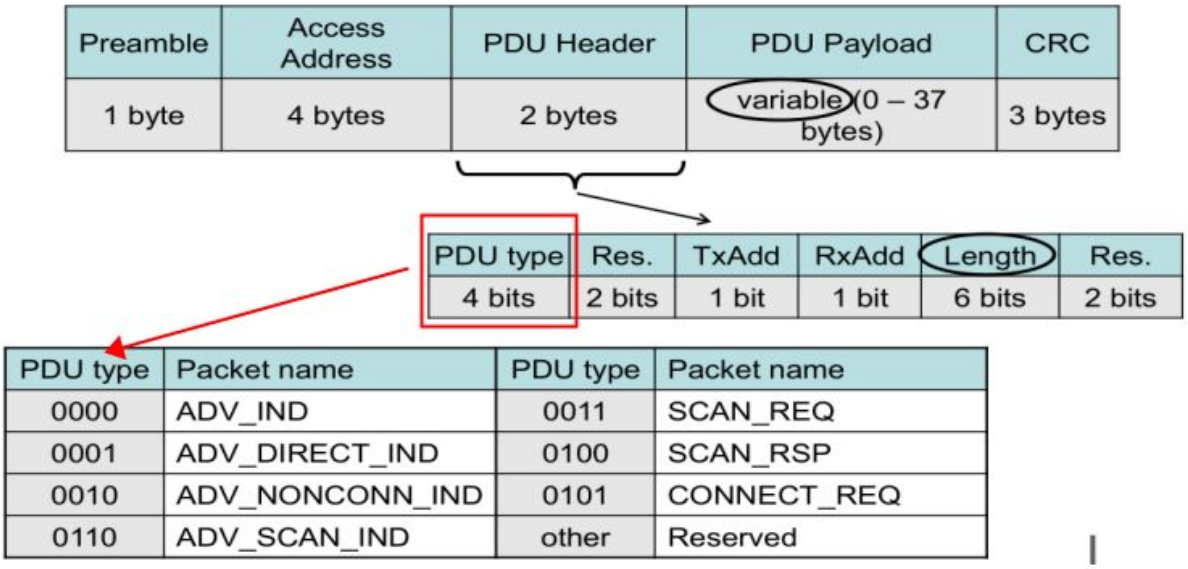
2)数据信道：提供给已经建立蓝牙连接的 master 和 slave 端提供可靠的数据通信信道。 BLE 规定，数据信道有 37 个。为加强通讯的可靠性，避开干扰， BLE 设备通过自适应跳频的方式在这 37 个信道上传。



第 4 部分：Access Address： 0xBE89BED6。所有 BLE 设备的广播帧都是使用这个地址，无论厂

家。

第 5 部分：



Preamble	Access Address	PDU Header	PDU Payload	CRC
1 byte	4 bytes	2 bytes	variable (0 – 37 bytes)	3 bytes

PDU type	Res.	TxAdd	RxAdd	Length	Res.
4 bits	2 bits	1 bit	1 bit	6 bits	2 bits

PDU type	Packet name	PDU type	Packet name
0000	ADV_IND	0011	SCAN_REQ
0001	ADV_DIRECT_IND	0100	SCAN_RSP
0010	ADV_NONCONN_IND	0101	CONNECT_REQ
0110	ADV_SCAN_IND	other	Reserved

PDU type 广播类型：例子为普通可连接广播。

A) 以 ADV_开头的帧表示该帧是广播帧，是由 advertiser(蓝牙外设)发出的，它们有 4 种类型，分别用在不同的蓝牙设备上面。

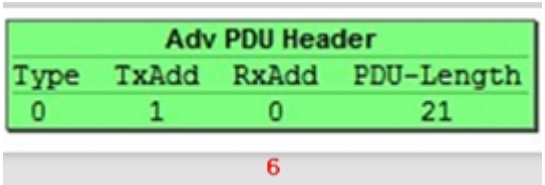
- ADV_IND:通用的可以建立连接的广播， nRF51822 通常发送这种广播。
- ADV_DIRECT_IND:快速广播。广播最长发射时间为 1.28S。
- ADV_NONCONN_IND:不能建立连接的广播信号, ibeacon 发的就是这种类型的广播

B) ADV_SCAN_IND 为扫描帧，是由 scanner（手机、平板、 PC）发出的。

C) ADV_SCAN_REQ 为扫描请求帧， 是由 scanner（手机、平板、 PC）发出的。 只在 scanner 想从 advertiser 获取更多的广播数据的时候才由 scanner 发出。相应的，当 ADV_SCAN_REQ 被发出以后， advertiser
会以 SCAN_RSP 作为回应。

D) SCAN_RSP 为 ADV_SCAN_ REQ 的回应。

E) CONNECT_REQ 为 scanner 向 advertiser。



Adv PDU Header			
Type	TxAdd	RxAdd	PDU-Length
0	1	0	21

第 6 部分：

•TxAdd、 RxAdd 用来表示发送该广播帧的蓝牙设备的蓝牙地址类型。 1 表示 random address 0 表示 public address。 蓝牙地址的种类。

蓝牙协议规定，任何一个蓝牙设备必须拥有一个唯一的 48 bit 的地址，用以标识标识身份。而且，在广播的时候必须要把蓝牙地址广播出去。蓝牙地址有以下的四种:

1)Public address.

Public address 是公司通过 IEEE 申请获得的,称为 OUI(Organizationally Unique Identifier)。这 个地址是固定的地址，全球唯一的，不可以修改。

Public address 的 24 bit LSB 用来表示公司名；另外 24 bit 的 MSB 用来分配给不同的产品类型。

2) Random Static address

Random Static address 是设备在上电的时候随机生成或者是芯片厂家在生产芯片的时候随 机烧录的不重复的 48 bit 的蓝牙地址。 nRF51822 的蓝牙地址属于后者。该地址存放在 FICR 里 面，用户不可以修改。

6.2.13 DEVICEADDR[0]

Bit number	31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
ID (Field ID)	A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A
Value after erase	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

ID	RW	Field	Value ID	Value	Description
A	R	ADDR			Device address bit 31-0.

6.2.14 DEVICEADDR[1]

Bit number	31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
ID (Field ID)	- - - - - - - - - - - - - - - - A A A A A A A A A A A A A A A A
Value after erase	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

ID	RW	Field	Value ID	Value	Description
A	R	ADDR			Device address bit 47-32.

Random Static address 的最高位的后 2 bit 必须要为 1 。

3)Private Non-Resolvable address 和 Private Resolvable address

这 2 种地址不常用 ，这里就不介绍了。

nRF51822 采用的是 Random Static address， 在启动的时候协议栈从 FICR 里面读取作为设备的蓝牙 地址.如果用户需要使用 Public address,则需要使用 sd_ble_gap_address_set()这个函数重新设定蓝牙地址。本例广播包是从设备 TxAdd 为 1，也就是设置为了 Random Static address

•Length 表示后面 PDU Payload 的大小。

AdvA
0xE11D2123261C

7

第 7 部分： 蓝牙设备地址，也可以尝试自己读取一下 FICR 里面的蓝牙地址跟抓包得到的对比一下，看是否是一样的。

AdvData									
0E	09	4C	65	64	42	75	74	74	6F	6E
44	65	6D	6F	03	19	34	12	02	01	05

8

第 8 部分：

PDU Payload 中 “0E 09 4C 65 64 42 75 74 74 6F 6E 44 65 6D 6F”为一 组。 0E 为本字段长度； 09 为 LOCAL NAME， 也就是蓝牙设备名称。通过查找 ASCII 码表，我们可 以得到它的蓝牙设备名称为 ”Nordic_HRM”。读者 可以在 BLE 实验二：BLE LED 灯读写控制的项目工程中中找到其定义，如下所示。读者应该知道以后是在这个地方改蓝牙设备的名称了。

4C->L 65->e 64-> d 42-> B 75->u 74-> t 74 ->t 6F-> o 6E-> n 44->D 65->e 6D->m 6F->o

```
#define CONNECTED_LED_PIN_NO            LED_1                                   /**< Is on when devic

#define LEDBUTTON_LED_PIN_NO            LED_0
#define LEDBUTTON_BUTTON_PIN_NO         BUTTON_1

#define DEVICE_NAME                     "LedButtonDemo"                         /**< Name of devi

#define APP_ADV_INTERVAL                64                                      /**< The advertis
#define APP_ADV_TIMEOUT_IN_SECONDS      180                                     /**< The advertis

#define APP_TIMER_PRESCALER             0                                       /**< Value of the
#define APP_TIMER_MAX_TIMERS            2                                       /**< Maximum numb
#define APP_TIMER_OP_QUEUE_SIZE         4                                       /**< Size of time
```

“03193412”为一 组。 03 为本字段长度;19 为 APPEARANCE，因为蓝牙发送数据是低位在前，所 以 ”3412”其实是”1234”， 0x1234 转换成十进制就是 4660,。 APPEARANCE 这个 AD TYPE 是新添加的 TYPE，所以在 CORE4.0 核心协议里面是找不到的，这个在代码里认为是 UNKOWN

```
#define BLE_APPEARANCE_UNKNOWN                              0   /**< Unknown. */
#define BLE_APPEARANCE_GENERIC_PHONE                        64  /**< Generic Phone. */
#define BLE_APPEARANCE_GENERIC_COMPUTER                     128 /**< Generic Computer. */
#define BLE_APPEARANCE_GENERIC_WATCH                        192 /**< Generic Watch. */
#define BLE_APPEARANCE_WATCH_SPORTS_WATCH                   193 /**< Watch: Sports Watch. */
#define BLE_APPEARANCE_GENERIC_CLOCK                        256 /**< Generic Clock. */
#define BLE_APPEARANCE_GENERIC_DISPLAY                      320 /**< Generic Display. */
#define BLE_APPEARANCE_GENERIC_REMOTE_CONTROL               384 /**< Generic Remote Control. */
#define BLE_APPEARANCE_GENERIC_EYE_GLASSES                  448 /**< Generic Eye-glasses. */
#define BLE_APPEARANCE_GENERIC_TAG                          512 /**< Generic Tag. */
#define BLE_APPEARANCE_GENERIC_KEYRING                      576 /**< Generic Keyring. */
#define BLE_APPEARANCE_GENERIC_MEDIA_PLAYER                 640 /**< Generic Media Player. */
#define BLE_APPEARANCE_GENERIC_BARCODE_SCANNER              704 /**< Generic Barcode Scanner. */
#define BLE_APPEARANCE_GENERIC_THERMOMETER                  768 /**< Generic Thermometer. */
#define BLE_APPEARANCE_THERMOMETER_EAR                      769 /**< Thermometer: Ear. */
#define BLE_APPEARANCE_GENERIC_HEART_RATE_SENSOR            832 /**< Generic Heart rate Sensor. */
#define BLE_APPEARANCE_HEART_RATE_SENSOR_HEART_RATE_BELT    833 /**< Heart Rate Sensor: Heart Rate Belt. *
#define BLE_APPEARANCE_GENERIC_BLOOD_PRESSURE               896 /**< Generic Blood Pressure. */
#define BLE_APPEARANCE_BLOOD_PRESSURE_ARM                   897 /**< Blood Pressure: Arm. */
#define BLE_APPEARANCE_BLOOD_PRESSURE_WRIST                 898 /**< Blood Pressure: Wrist. */
#define BLE_APPEARANCE_GENERIC_HID                          960 /**< Human Interface Device (HID). */
#define BLE_APPEARANCE_HID_KEYBOARD                         961 /**< Keyboard (HID Subtype). */
#define BLE_APPEARANCE_HID_MOUSE                            962 /**< Mouse (HID Subtype). */
```

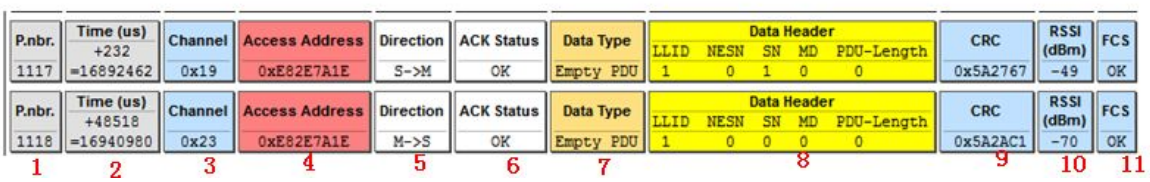
“020105”为一 组。 02 为本字段长度; 01 是 FLAGS, 06 表示本设备只支持 BLE，不支持传统蓝牙。 05 的取值其实为 04+01，看下图可以明白。

Value	Description	Bit	Information
0x01	Flags	0	LE Limited Discoverable Mode
		1	LE General Discoverable Mode
		2	BR/EDR Not Supported (i.e. bit 37 of LMP Extended Feature bits Page 0)
		3	Simultaneous LE and BR/EDR to Same Device Capable (Controller) (i.e. bit 49 of LMP Extended Feature bits Page 0)
		4	Simultaneous LE and BR/EDR to Same Device Capable (Host) (i.e. bit 66 of LMP Extended Feature bits Page 1)
		5..7	Reserved

1.2 数据包抓取：

当开发板 一旦和主机连接上后， 到这一行， 抓包就不在显示了， 这个时候， 如上填入地址，并选好信道号：

然后再重新复位从机，主机重新连接，这个时候不一定 SmartRF Packet Sniffer 就能显示到连接后的数据包。如果不能连接上， 就试试把 信道改成 38、 39 等等， 多试试几次， 就会出现下面图了。（下图表明抓取到了 ble 的数据包）



前 3 个就不说明了，和广播包的一样。第四个 Access Address 为数据接入地址，接入地址由主设

备来提供，地址通过随机生成。但是也要遵循一定规律。不同与广播接入地址固定，具体规律大家可以查蓝牙协议，这里不展开了。

第 5 个：为连接方向，是主机到从机，还是从机到主机。

第 7 个：数据类型。

第 8 个：报头，如下图所示说明：

Preamble	Access Address	PDU Header	PDU Payload	CRC
1 byte	4 bytes	2 bytes	variable (0 – 37 bytes)	3 bytes

LLID	NESN	SN	MD	Res.	Length	Res.
2 bits	1 bit	1 bit	1 bit	3 bits	5 bits	3 bit

LLID	Packet type
00	Reserved
01	LL Data PDU: continuation fragment of an L2CAP message or empty PDU
10	LL Data PDU: start of an L2CAP message
11	LL Control PDU

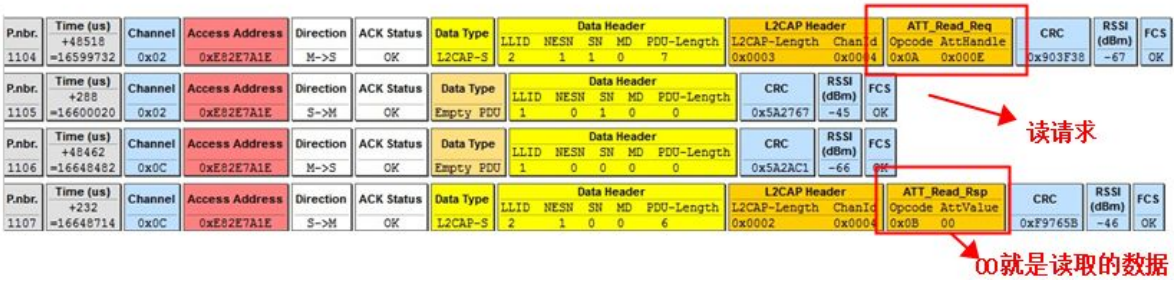
ata bit

11：链路层控制报文：用于管理连接

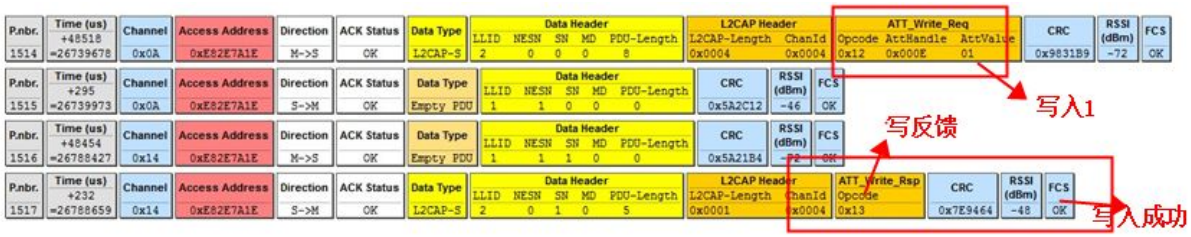
10：高层报文开始：可用于一个完整报文

01：高层报文延续

NESN:下一个预期序列号。SN：序列号。MD:更多数据。PDU-Length:PDU 长度。没有同学的 PDU 数据长度为 0，如果我们通信一下，使用例子二：ble 的 LED 读写，读操作如下：



如果通过手机 MCP 写入一个 01，抓包如下：



在实际开发中，为了确定你的数据或者连接是否正确，抓包还是显得比较重要的，所以十分建议大家配一个抓包器进行开发。

重要的参考文档：

文档	描述
nRF51822 Evaluation Kit User Guide	使用 Evaluation Kit 开发板的介绍和配置，包括 Keil 和 SoftDevice 的配置。
nRF51 SDK documentation	这个文件在 SDK 安装的文件夹之下的子文件夹中，包含了 SDK 中所有功能 API 的文档。
S110 nRF51822 SoftDevice Specification	介绍了协议栈 S110 SoftDevice，包括资源的用法和高级的功能函数。
nRF51822 Product Specification	描述了 nRF51 的硬件、模块和电气特性。
nRF51 Series Reference Manual	介绍了 nRF51 芯片系列所有功能模块的描述和芯片所有的外围资源。
nAN-15: Creating Applications with the Keil C51 Compiler	这个应用手册包含使用 Keil µVision 的信息，它为 nRF24LE1 芯片而写，但是 3.3 节“Including files”和 3.4 节““Debug your project”同样适用于 nRF51822 芯片。
Bluetooth Core Specification, version 4.0 卷 1,3,4,6	这个文档由蓝牙技术联盟组织提供，包含了关于蓝牙服务和 profiles 的信息。