2.4G模拟BLE的广播理论基础

笔记本： 2.4G技术
创建时间： 2016/2/20 14:23 更新时间： 2016/4/29 14:18
作者： 404267906@qq.com

这个附件为基于STM32 正点原子的开发板

模拟的理论基础。

BLE的广播

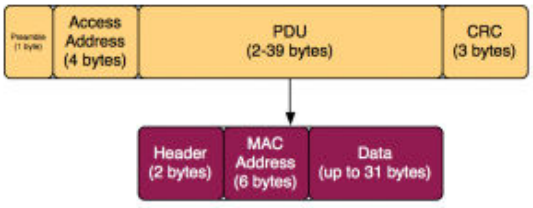
广告（Advertising）是一种单向的发送机制。想要被搜索到的设备可以以20毫秒到10秒钟的时间间隔发送一段数据包。使用的时间间隔越短，电池消耗的越快，但设备被发现的速度也就会快。数据包长度最多47个字节，由以下部分组成：

1 byte preamble（1字节做报头）

4 byte access address（4字节做地址）

39 bytes advertising channel PDU（39个字节用于PDU数据包）

3 bytes CRC（3个字节用于CRC数据校验）



- 在NRF24的payload使用的可以定义为
-
- 其中payload是按照btle_pdu_chunk。在demo简单实现所以直接使用buf进行，未使用这个结构体形式表现。

BLE的工作是在1Mbps使用在nrf24L01的也需要在该速率上实现。
在广播事件中是在37、38、39即如下图
其中在射频对应频率
所以在NRF24的设置为2402、2426、2480。
即在代码中为
static const uint8_t chRf[] = { 2, 26, 80 };
static const uint8_t chLe[] = { 37, 38, 39 };
需要注意的在代码“简化”在广播的间隔时间。

对于广告通信信道，地址部分永远都是 `0x8E89BED6` 。对于其它数据信道，地址部分由不同的连接决定。

返回的PDU数据也拥有自己的数据报头（2个字节：声明有效载荷数据的长度和类型——设备是否支持连接等等）和当前有效载荷数据（最多37个字节）。

最终，有效载荷数据中的头6个字节是设备的MAC地址，所以实际信息数据最高可占31个字节。

现在我们来看看我们使用是NRF24L01的shockburst模式。

7.9.1 ShockBurst™ packet format

Figure 25. shows the packet format with MSB to the left.

Preamble 1 byte	Address 3-5 byte	Payload 1 - 32 byte	CRC 1-2 byte

Figure 25. A ShockBurst™ packet compatible with nRF2401/nRF2402/nRF24E1/nRF24E2 devices.

与上图简单对比我们可以发现他们之间很类似。但是有些地方差异。

- adder是需要设置为4位，并且固定为0x8E89BED6。
- 由于BLE的CRC是使用的是CRC 24bit。这部分是需要我们进行关闭NRF24的CRC的硬件，使用软件算法实现这个CRC24的。

3.1.1 CRC 产生

所有链路层的数据包都需要计算 PDU 的 CRC。如果 PDU 是加密的，则先加密后进行 CRC 计算。

CRC 多项式是一个 24 位的 CRC，并且 PDU 从最低位起所有位都需要参与计算。多项式为：

$$x^{24} + x^{10} + x^9 + x^6 + x^4 + x^3 + x + 1$$

对于所有数据信道的 PDU，CONNECT_REQ PDU 中链路层的通信与连接中所有的移位寄存器被设置为 CRC 初始值，每一个广播信道的 PDU，移位寄存器被设置为 0x555555。

CRC 传输时从最高位 bit23 开始传输。

下图描述了如果产生一个 CRC：

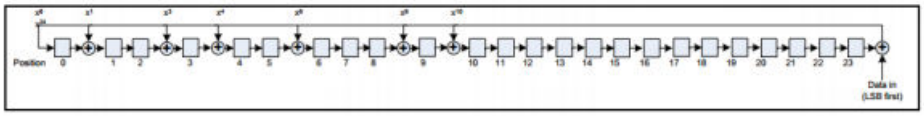


Figure 3.2: The LFSR circuit generating the CRC

- 同时在BLE的时候实用到**whitening白化。【可以参考<低功耗蓝牙开发权威指南>第7章】**

3.2 数据白化

数据白化是为了避免数据流中长序列的 0 或 1，链路层数据包中的 PDU 及 CRC 都需要数据白化，并且数据白化的执行在 CRC 运算之后。接收方解数据白化执行在 CRC 运算之前。

数据白化与解白化使用相同的方式，使用了一个 7 位的线性反馈移位寄存器，其多项式为

$$x^7 + x^4 + 1$$

在数据白化与解白化之前，移位寄存器需要被初始化，初始化值是具有以下格式，并且由数据包传输的信道索引推导而来：

- 位 0 为 1
- 位 1-6 设置为收发时所使用的信道索引，位 1 为最高有效位，位 6 为最低有效位。

如信道索引为 23=0X17=1110 101B。

下图显示了数据白化的产生：

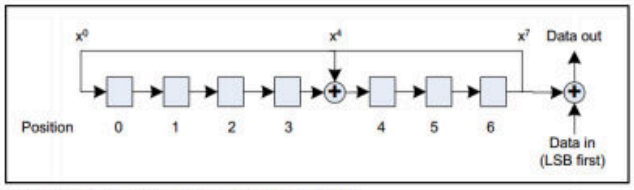
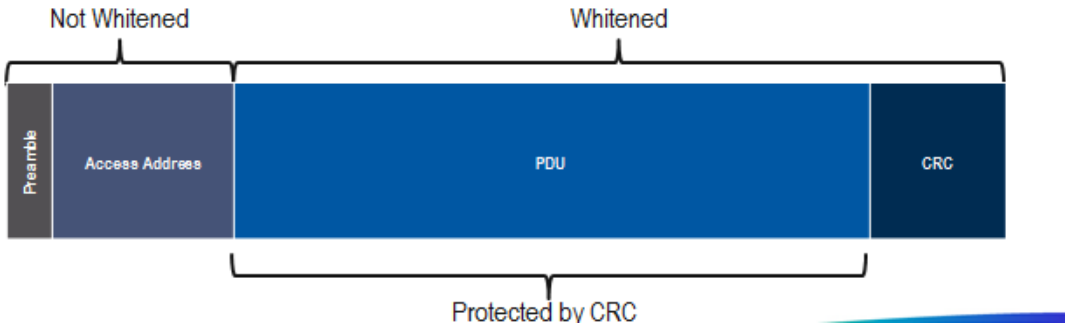


Figure 3.3: The LFSR circuit to generate data whitening

- 其中白化和CRC的作用范围如下

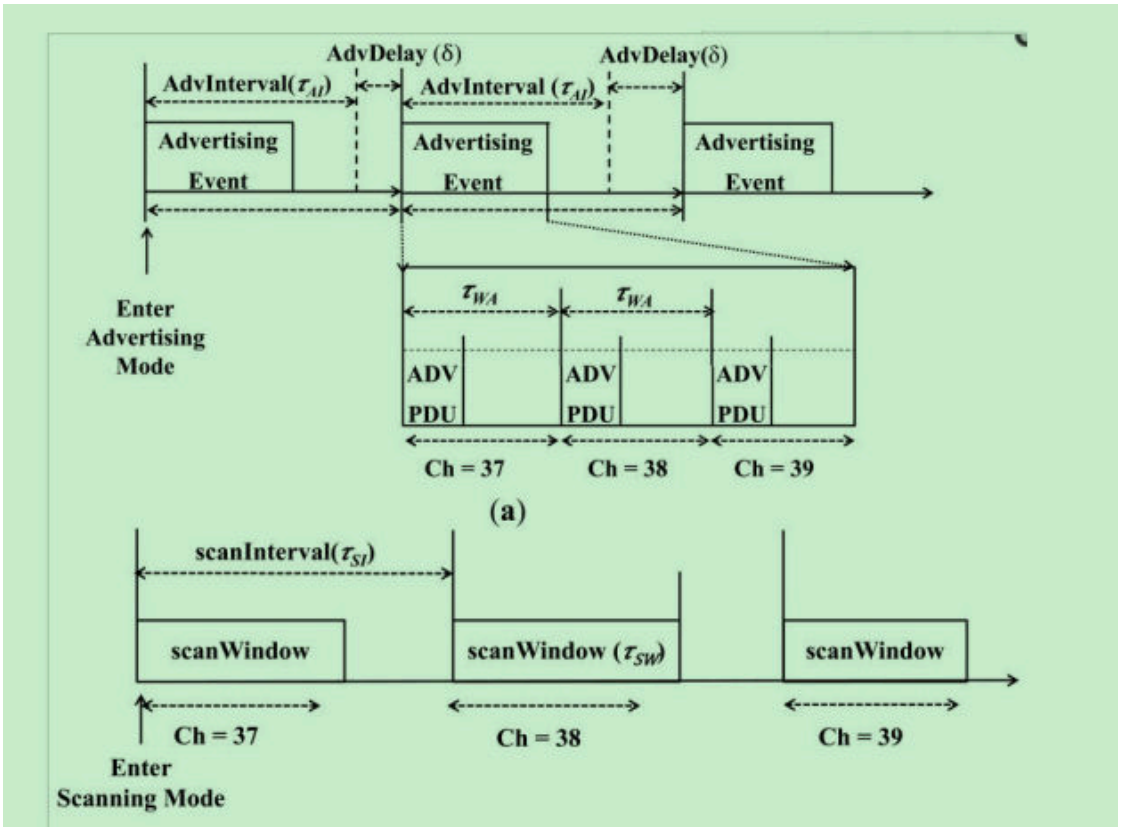


- 在NRF24的payload使用的可以定义为

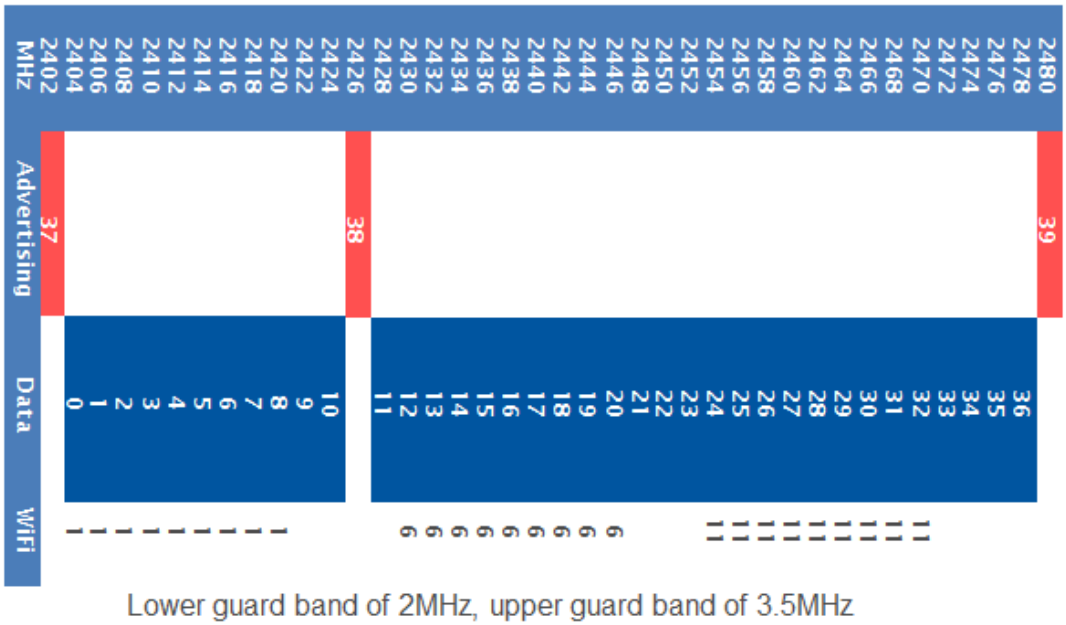
```
// advertisement PDU
struct btle_adv_pdu {

    // packet header
    uint8_t pdu_type; // PDU type
    uint8_t pl_size;  // payload size
    // MAC address
    uint8_t mac[6];
    // payload (including 3 bytes for CRC)
    uint8_t payload[24];
};

// payload chunk in advertisement PDU payload
struct btle_pdu_chunk {
    uint8_t size;
    uint8_t type;
    uint8_t data[];
};
```

其中payload是按照btle_pdu_chunk。在demo简单实现所以直接使用buf进行，未使用这个结构体形式表现。

BLE的工作是在1Mbps使用在nrf24L01的也需要在该速率上实现。
在广播事件中是在37、38、39即如下图



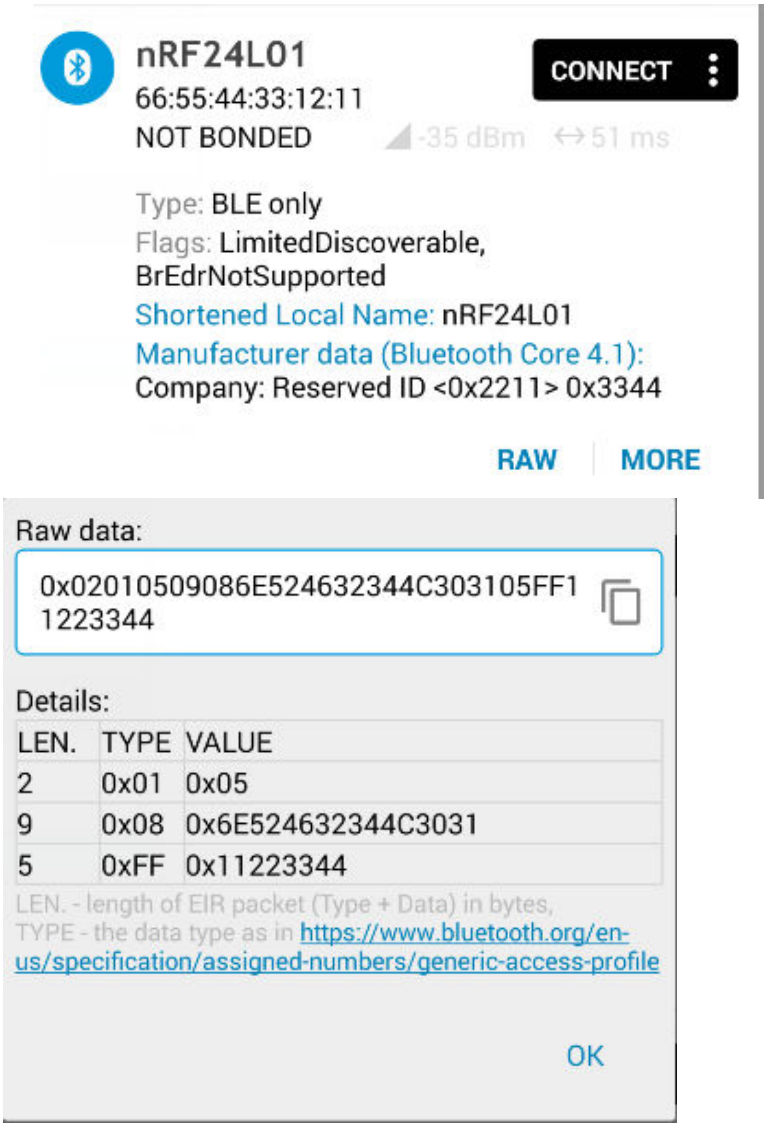
其中在射频对应频率



所以在NRF24的设置为2402、2426、2480。
即在代码中为

```
static const uint8_t    chRf[] = { 2, 26, 80 };
static const uint8_t    chLe[] = { 37, 38, 39 };
```

需要注意的在代码“简化”在广播的间隔时间。


nRF24L01
66:55:44:33:12:11
NOT BONDED
CONNECT
-35 dBm
51 ms
Type: BLE only
Flags: LimitedDiscoverable, BrEdrNotSupported
Shortened Local Name: nRF24L01
Manufacturer data (Bluetooth Core 4.1):
Company: Reserved ID <0x2211> 0x3344
RAW
MORE
Raw data:
0x02010509086E524632344C303105FF1 1223344
Details:
LEN. TYPE VALUE
2 0x01 0x05
9 0x08 0x6E524632344C3031
5 0xFF 0x11223344
LEN. - length of EIR packet (Type + Data) in bytes,
TYPE - the data type as in https://www.bluetooth.org/en-us/specification/assigned-numbers/generic-access-profile
OK


Mini STM32
NRF24L01 TEST
ATOM@ALIENTEK
2011/7/1
24L01 Ready!
NRF24L01 Beacon
ALIENTEK
MiniSTM32
V2.0
ALIENTEK TFTLCD

其他的资料