OTA 升级简要说明

第一步：安装 OTA 程序

第二步：在手机上打开这个程序

这张图上，你能看到 5 个模块，每个有数字标识

第一个模块： 要升级的目标 bin 文件

描述：选择要升级的目标 bin 文件所在的目录

第二个模块：蓝牙设备列表中列举当前处于广播状态的所有蓝牙设备

描述：从蓝牙设备列表中选择你要升级的设备

第三个模块： 刷新蓝牙列表

描述：按下这个按键，你就能重新刷新当前处于广播状态的所有蓝牙设备

第四个模块： 开始 OTA 空中升级

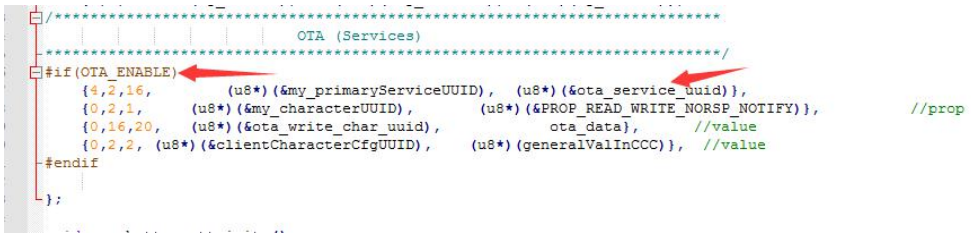
描述：点击这个按键就能触发 OTA 事件。

第五个模块： 显示当前状态

描述： 这步骤显示了 OTA 事件的进度。

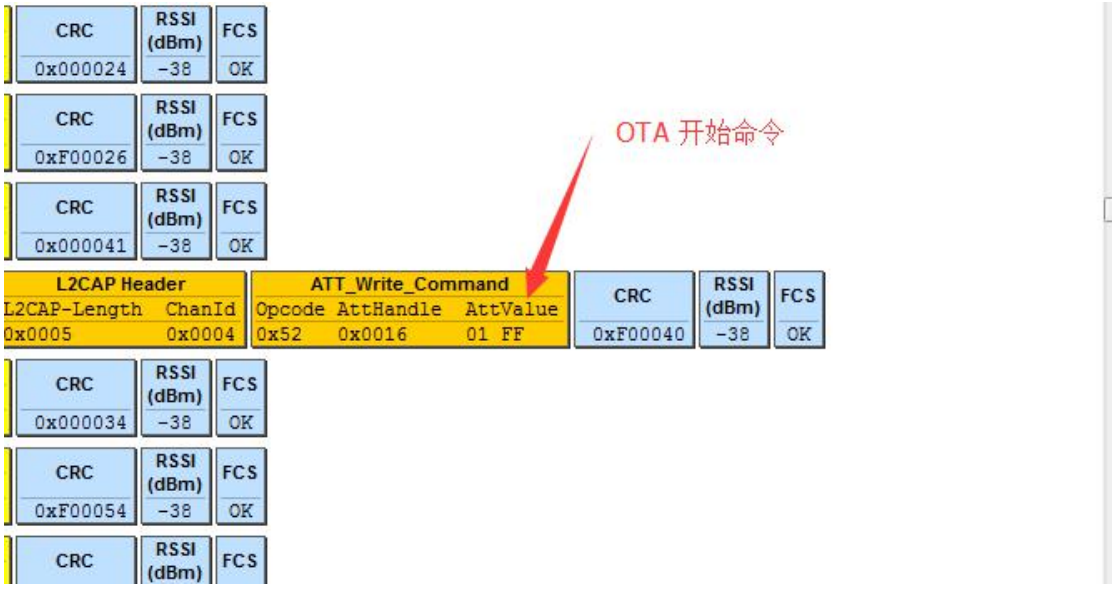
实现的细节：

1．要使用 OTA 功能，首先要在 attribute list 中使能 OTA 的 attribute.



2. ota_master 通过 RF 将 New_firmware.bin 空运给 Slave

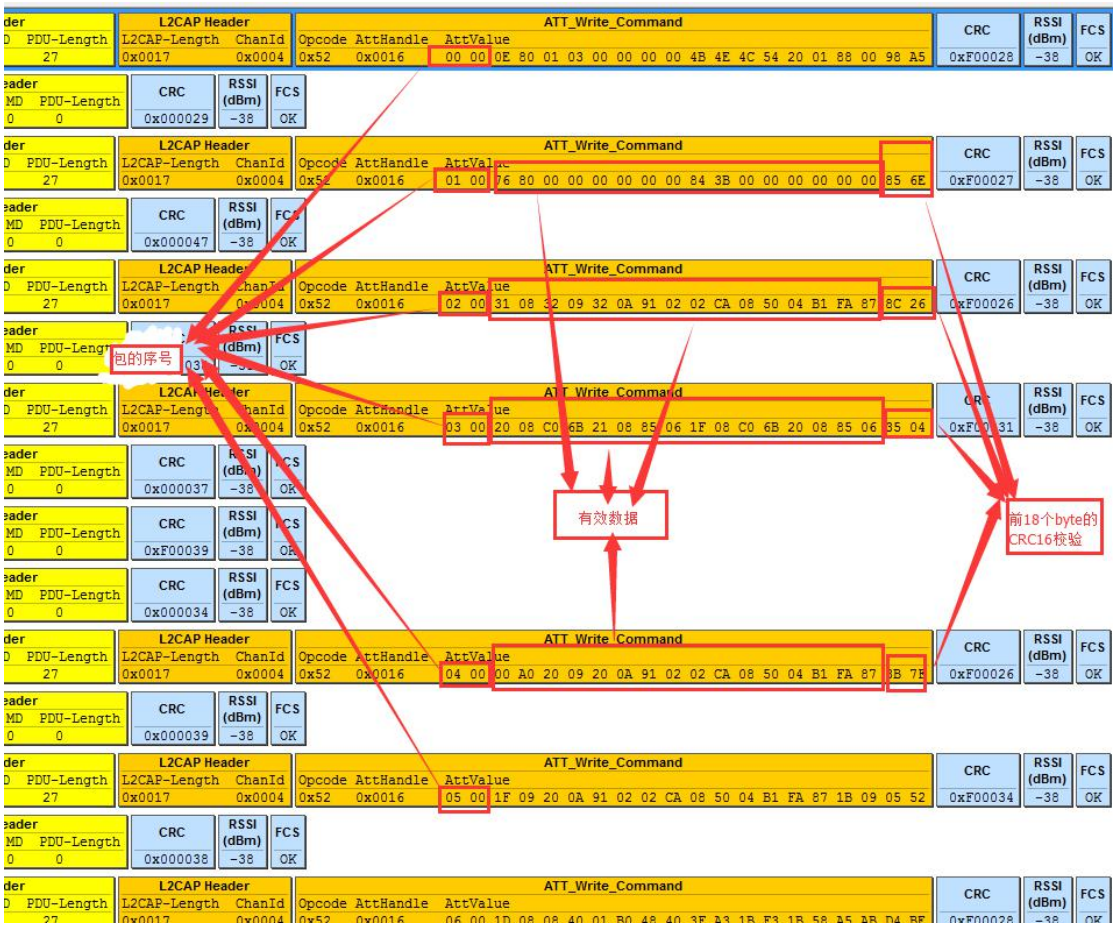
二者都进入 OTA 模式后 ,ota_master 发送带有 New_firmware 数据的 OTA data 包，Slave 收到包并解析 将数据烧写到 flash 的 0x20000~0x40000 新 firmware 存储区。



3.APP 通过 ATT_OP_WRITE_CMD （0x52）命令发送数据包到从设备，数据格式如下

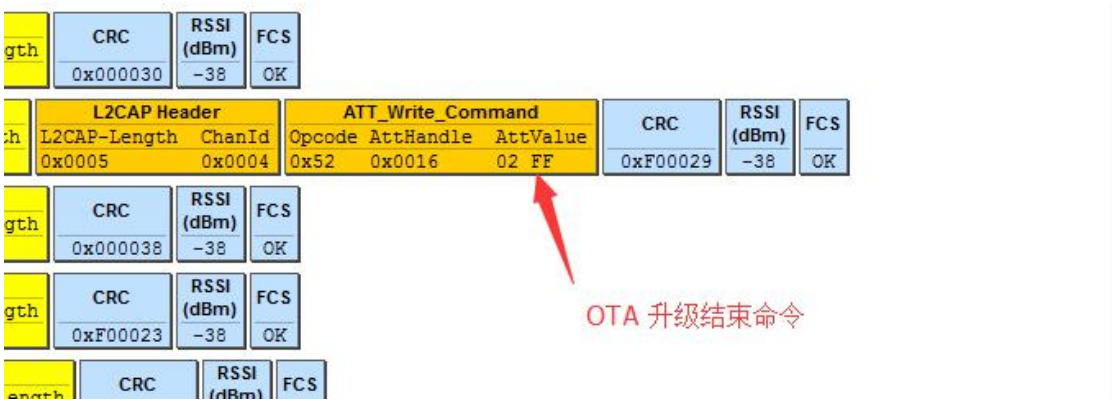
Data[23]	Description
0~1	SerialNumber(start from 0x0000)
2~17	16byte data of new bin file
18~19	CRC Value of previous 18 bytes
20~22	Reserved

4. OTA 升级过程抓包如下：



5. OTA data 发送完毕后，ota_master 发送 OTA end 命令 “0xff02” ，Slave reboot。

当整个 OTA 过程顺利完成后，此时 New_firmware.bin 已经存储在 Slave 的 0x20000~0x40000。Slave 将 flash 0x73000 上的 boot_flag 的值设置为特定的 0xa5，然后 reboot MCU。



接下来在从设备中的情况如下：

1）slave 运行 ota_boot.bin

slave reboot 后，MCU 将 flash 0x00000 地址处的 Old_firmware.bin 中前一部分指令搬到 SRAM 从 0x808000 开始的地方，运行 Old_firmware.bin 中 cstartup.S 对应的启动代码，该启动代码对 flash 0x73000 上的 boot_flag 的值做检测，发现该值是 0xa5，这时候不再运行正常的 Old_firmware.bin 对应的代码，而是将 flash 0x72000~0x72600 区域 1.5K 的 ota_boot.bin 搬到 SRAM 0x808000~0x808600 的地方，搬移完成后，reset MCU（reset 只是让 MCU 从 SRAM 0x808000 地址开始运行，不会重新从 flash 搬代码到 SRAM 中）。此时 MCU 从 0x808000 处开始重新运行，相当于运行了 ota_boot.bin 的功能。

1) ota_boot 更新代码，reboot

ota_boot.bin 运行后，从 flash 0x20000 开始的地方逐页读取 New_firmware.bin 的内容，并写到 flash 0x00000 开始的对应地址处，相当于将 New_firmware.bin 完全更新到 flash 0 地址处。更新完成后，将 flash 0x73000 上的 boot_flag 的值设定为 0x00，reboot MCU。

2) New_firmware.bin 正常运行

MCU 再次 reboot 后，从 flash 0 地址搬代码到 SRAM 0x808000 开始的地方，并且检测到 boot_flag 的值不是 0xa5，启动正常的 slave 功能，该 New_firmware.bin 类似于之前的 Old_firmware.bin，也具有 OTA 功能，可以再次启动 OTA 模式更新代码（最新的代码要重新下载到 ota_master 的 flash 0x20000 地址处）。