
三通道开关 BLE 通讯协议

版本：____V0.5____

制定：_____

审核：_____

批准：_____

版本修订记录			
版本号	修订描述	修订人/日期	批准人/日期
V0.1	草稿	吴蜜 2020.04.14	
V0.2	1. 补充延时操作的细节。	吴蜜 2020.04.14	
V0.3	1. 删除与协议无关，仅与具体设备功能实现相关的描述。	吴蜜 2020.04.15	
V0.4	1. 更正错误的控制命令示例。	吴蜜 2020.05.11	
V0.5	1. 更正错误的延时控制示例；补充步长为 5 分钟的描述。	吴蜜 2020.05.13	

目录

一. 概述..... 4

二. 系统拓扑..... 4

三. 绑定解绑流程..... 4

四. 通讯协议..... 5

 1. 字节序..... 5

 2. BLE ADV_NONCONN_IND 格式..... 5

 3. 控制数据 AdvData 格式..... 5

 4. 字段含义..... 6

 5. 数据加密..... 7

 6. 控制命令示例: 7

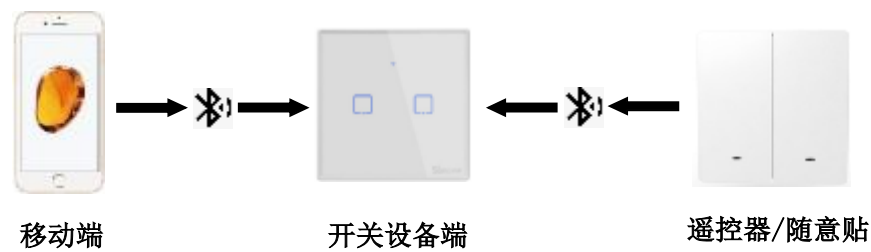
五. 附录..... 8

一. 概述

该文档定义了现阶段 BLE 开关在实际应用中的通讯协议。

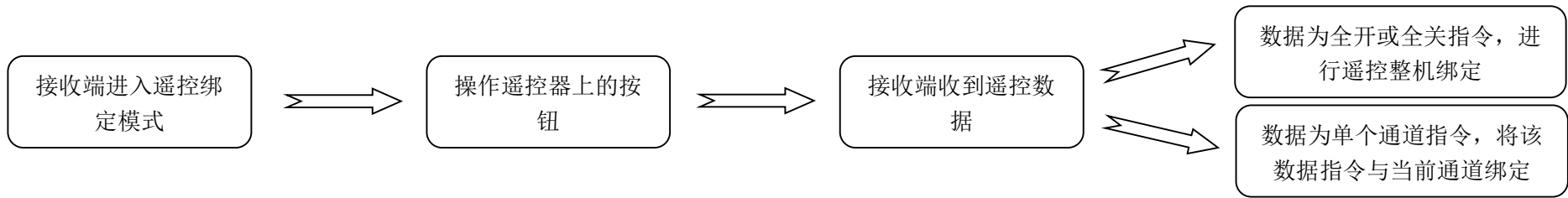
二. 系统拓扑

以下拓扑描述了现阶段 BLE 开关应用在智能家居中的应用连接关系，其中箭头方向表明数据通讯方向。



三. 绑定解绑流程

在该应用中，遥控端与接收端的绑定关系分为单键单通道绑定和遥控设备与接收设备整机绑定，二者是以遥控端不同按键的操作进行区分。如在绑定模式时，遥控端操作的为具体的某个通道控制按键，则进行单键单通道绑定，绑定是以当前接收到的遥控按键指令与当前由接收设备进入绑定模式的按键通道进行绑定；如在绑定模式时，遥控端操作的是全开或全关按键，则进行遥控设备与接收设备整机绑定；



单键单通道绑定：仅已绑定的遥控按键可操作接收设备被绑定的通道。

整机绑定：当进行了整机绑定后，遥控设备上所有的按键可控制接收设备对应的通道，该对应关系固定(下述协议中，Para 字段 Byte1，遥控端和接收端一一匹配，0x00 对应 0x00，0x01 对应 0x01，0x02 对应 0x02)。

同一接收设备在与同一遥控绑定时，只能存在一种绑定关系，要么是单键单通道绑定，要么是整机绑定，当前绑定关系会覆盖上一次绑定关系。

四. 通讯协议

该数据通信使用 BLE 广播包的方式，遵循蓝牙规范 4.0，使用 ADV_NONCONN_IND 广播包。

1. 字节序

对于多字节的字段，均采用小端模式，即低位优先。值已固定的多字节字段，已采用小端字序。

2. BLE ADV_NONCONN_IND 格式

Field	Preamble(固定)	Access Address(固定)	Header	AdvA	AdvData	CRC
Size(octets)	1	4	2	6	0-31	3
Value	0xAA	0xD6, 0xBE, 0x89, 0x8E				

其中 Preamble，Access Address 固定，Header，AdvA，AdvData 和 CRC 根据情况填写，控制数据在 AdvData 中。

3. 控制数据 AdvData 格式

Filed	AD Structure 1	AD Structure 2 [28 Octs]													
Ctrl Filed		Len	AD Type	Comp ID	Fixed	Type	Version	Count	Addr	Group	Cmd	Para	RFU	Rand	Crc
Size(octets)	3	1	1	2	6	1	1	1	4	1	1	3	3	1	2
Value	0x02, 0x01, 0xXX	0x1B	0x05/0x03	0xFF, 0xFF	0xEE,0x1B, 0xC8,0x78, 0xF6,0x4A										

4. 字段含义

- ◆ **AD Structure 1:** 为手机发 BLE ADV 默认字段，手机系统自动添加，0xXX 根据手机类型有差异；在遥控器端 0xXX 固定为 0x02。
- ◆ **Len:** 为 AD Type 到 Crc 总长度，目前固定为 0x1B。
- ◆ **AD Type:** 由于 IOS 和安卓平台差异，具体值根据平台提供的 API 而定；遥控器建议使用 0x05。
- ◆ **Comp ID:** 固定为 0xFF, 0xFF。
- ◆ **Fixed:** 固定，使 MCU 端能顺利接收到数据，值为：0xEE, 0x1B, 0xC8, 0x78, 0xF6, 0x4A（小端模式）。
- ◆ **Type:** 标识类型，灯/风扇灯/浴霸或其他类型的家居。

协议中已支持的设备

设备类型	灯	风扇	风扇灯	浴霸	开关	其它
参数	0x01	0x02	0x03	0x04	0x05	0x06 - 0xFF

- ◆ **Version:** BIT0-6 用于标识版本号，BIT[7]用于标识 APP/REMOTER。

位	Bit7		Bit6 - Bit0
参数	0	1	xxxxxxx
含义	REMOTER	APP	表示版本号

- ◆ **Count:** 用于标识新旧数据，每发一条新指令，需要+1。
- ◆ **Addr:** 用于绑定和标识不同的 APP/遥控器，APP 使用 PUBLIC MAC ADDR 的低 4 字节，遥控器使用滚码。
- ◆ **Group:** 标识分组号，该应用分组目前为 0x01。
- ◆ **Cmd:** 控制命令，见下表：

*Cmd [1Byte] + Para [3Byte]			
功能	Cmd	Para	说明
开关	0x10	格式: [Byte2], [Byte1], [Byte0]; Byte2: 动作指令，开(0x01)、关(0x00)、翻转(0x02); Byte1: 指定开关通道号，范围为 0x00-0xFF，其中 0xFF 为全	示例: 第 0 通道即时关闭，指令：0x00, 0x00, 0x00; 第 1 通道即时打开，指令：0x01, 0x01, 0x00; 第 2 通道即时翻转，指令：0x02, 0x02, 0x00; 全部通道即时关闭，指令：0x00, 0xFF, 0x00;

		部通道; Byte0: 延时时间, 取值范围 0x00-0xFF, 该参数步长为 5 分钟, 其中 0x00 为即时;	全部通道即时打开, 指令: 0x01, 0xFF, 0x00; 第 0 通道延时 30 分钟关闭, 指令: 0x00, 0x00, 0x06;
--	--	---	--

- ◆ **Para:** 控制参数, 根据控制命令有差异, 见 Cmd 参数表格。
- ◆ **RFU:** 暂时未使用, 用于后续扩展或鉴权使用。
- ◆ **Rand:** 随机数, 每次发新数据 (Count++) 均需要重新生成。
- ◆ **Crc:** 用于校验数据的准确性, 使用 CRC16_CCITT 算法, 多项式: $x^{16} + x^{12} + x^5 + 1$, 初始值 0x5555, 范围从 Type 到 Rand 共 16 个字节。

5. 数据加密

为保证数据传输的相对安全, 采用如下方式对数据进行加密处理, 加密范围从 Type 到 Rand 共 16 个字节, 采用如下加解密方式:



- ◆ **明文:** 即未加密之前的原始数据。
- ◆ **A(Rand 加密):** 使用 Rand 对明文指定范围做字节 XOR 处理, 范围为 Group 到 RFU 共 8 字节。
- ◆ **B(EncodeTable 加密):** 使用 16 字节固定的 EncodeTable = {0x41, 0x92, 0x53, 0x2A, 0xFC, 0xAB, 0xCE, 0x26, 0x0D, 0x1E, 0x99, 0x78, 0x00, 0x22, 0x99, 0xDE}对 Type 到 Rand 共 16 字节做 XOR 处理, 该过程处理完成之后即可发送。
 - **B' (EncodeTable 解密):** 使用 16 字节固定的 EncodeTable = {0x41, 0x92, 0x53, 0x2A, 0xFC, 0xAB, 0xCE, 0x26, 0x0D, 0x1E, 0x99, 0x78, 0x00, 0x22, 0x99, 0xDE}对收到的数据的 Type 到 Rand 共 16 字节做 XOR 处理。
 - **A' (Rand 解密):** B' 解码之后得到 Rand, 使用 Rand 对 Group 到 RFU 共 8 字节做 XOR 处理。该过程处理完成之后即能得到完整的明文数据。

6. 控制命令示例:

第 0 通道开关即时翻转

说明	Comp ID	Fixed	Type	Version	Count	Addr	Group	Cmd	Para	RFU	Rand	Crc
明文	FFFF	EE1BC878F64A	05	02	E6	01010101	01	10	020000	000000	EA	5542
Rand 加密	FFFF	EE1BC878F64A	05	02	E6	01010101	EB	FA	E8EAEA	EAEAEA	EA	5542
EncodeTable 加密	FFFF	EE1BC878F64A	44	90	B5	2BFDAACF	CD	F7	F67392	EAC873	34	5542

第 0 通道开关即时打开

说明	Comp ID	Fixed	Type	Version	Count	Addr	Group	Cmd	Para	RFU	Rand	Crc
明文	FFFF	EE1BC878F64A	05	02	E6	01010101	01	10	010000	000000	EA	D79A
Rand 加密	FFFF	EE1BC878F64A	05	02	E6	01010101	EB	FA	EBEAEA	EAEAEA	EA	D79A
EncodeTable 加密	FFFF	EE1BC878F64A	44	90	B5	2BFDAACF	CD	F7	F57392	EAC873	34	D79A

全部道开关打开

说明	Comp ID	Fixed	Type	Version	Count	Addr	Group	Cmd	Para	RFU	Rand	Crc
明文	FFFF	EE1BC878F64A	05	02	42	01010101	01	10	01FF00	000000	65	1B99
Rand 加密	FFFF	EE1BC878F64A	05	02	42	01010101	64	75	649A65	656565	65	1B99
EncodeTable 加密	FFFF	EE1BC878F64A	44	90	11	2BFDAACF	42	78	7A031D	6547FC	BB	1B99

五. 附录

无。