JL 爱拍协议

V0.02

目录

修改日志

版本	日期	描述
0.0.1	2020/ 08 / 10	
更新：	● 建立初始版本 ● 定义文档格 ● 描述协议	

Chapter 1　JL 爱拍协议

1.1 概述

手机爱拍 APP 通过蓝牙 BLE 连接云台设备，通过发控制命令控制云台转动跟踪人脸拍照。并且同时可以控制设备 LED 的亮灭状态。手机爱拍 APP 同时支持安卓和苹果两个生态系统。

设计上支持 APP 和设备两者相向认证方式连接，保证匹配的可靠性。

1.2 广播包用户自定义数据

BLE 广播包分为 Advertising Data 包和 Scan Response Data 包。每个数据包最大是 31 Bytes。其中包含了设备类型，设备名称，厂商自定义数据等内容。

手机 APP 通过厂商自定义数据块来识别过滤设备，发起设备连接。厂商自定义数据块固定存放在 Advertising Data 包中，便于快速搜索。

数据定义格式

Offset (bytes)	Size (bytes)	备注说明
0	1	厂家自定义信息长度，固定值 0x19
1	1	信息类型，固定值 0xFF
2~3	2	杰理厂家 ID，固定值 0x05d6；小端存放，即为：D6 05
4~5	2	下级厂商 VID，小端存放
6~7	2	产品 PID，小端存放
8~14	6	ble 的 mac 地址低位先填入
15~18	4	随机数 FW_random，每次打开广播重新生成
19~26	8	FW_Hash1 值，低位先填入

Hash 值的生成方法：

把 16byte 的 USER_DATA 加 广播包中 12byte 的数据（定使用 offset 2~14 的数据）共 28 个 bytes，作为加密接口输入明文，offset 15~18 数据作为输入 key，调用算法加密后会输出 16 个 byte 加密数据，然后抽取其中前 8 个 byte 作为 FW_Hash1 值，让爱拍 APP 做设备识别，后 8 个 bytes 为 FW_Hash2 用于 APP 连接后发送给固件做认证识别。

App 通过同样的加密方法计算，验证 hash 值正确性，判断该广播包是否有效。

APP 根据下级厂商 VID 和 产品 PID（byte 4 ~ 7），区分产品类型。

USER_DATA：为 App 和固件约定相同的 16bytes 明文数据, SDK 发布默认值为全 FF，SDK 留接口给用户修改。

1.3 GATT 服务定义

//服务用于获取设备 GAP 名字

PRIMARY_SERVICE, 1800

CHARACTERISTIC, 2a00, READ | DYNAMIC,

//服务用于透传通信

PRIMARY_SERVICE, ab00

CHARACTERISTIC, ab01, WRITE | WRITE_WITHOUT_RESPONSE | DYNAMIC,

CHARACTERISTIC, ab02, NOTIFY ,

1.4 通信协议格式

手机 APP 和固件交换方式，协议数据内容均以小端方式存放。

1、发送包格式

Byte offset	描述	取值
0	CMD	0x01~0x7F
1	TAG	BIT7:代表是否需要应答，BIT0~BIT3:命令序号 SN,取值未（0x00~0x0f），其他 bit 默认为 0
2	length	Payload 的长度
3~?	Payload	

2、响应包格式

Byte offset	描述	取值
0	ACK	0xFF
1	ACK_CMD	应答的 CMD
2	ACK_TAG	BIT0~BIT3:为命令序号 SN，其他 bit 为 0
3	length	Payload 的长度
4~	Payload	

命令序号 SN：连接建立后初始值为 0，每发 1 条命令后，递增+1，范围 0x00~0x0f。

需要应答的时候，若超过 2 秒没有收到对方应答，走命令发送失败流程处理。

命令范围：

0x01~0x1f　认证命令

0x20~0x3f　控制命令

0x40~0x7f　保留未用

1.5 连接认证流程

爱拍 APP 连上设备后，APP 和设备都必须认证对方；如果认证通过，则允许控制协议执行，否则 APP 和固件都必现断开链路连接。

认证流程的数据流：

APP 使用 UUID ab01 的 WRITE_WITHOUT_RESPONSE 属性向固件发送数据。

固件使用 UUID ab02 的 NOTIFY 属性向 APP 发送数据。

APP 发送认证命令（500ms 超时重发，最多发 3 次）

Byte offset	描述	取值
0	CMD	0x01
1	TAG	0x80 + SN,需要应答
2	length	0x0C
3~11	Payload1	FW_Hash2，设备广播包加密生成 hash 值的后 8bytes
12~16	Payload2	APP_Random，app 每次发起连接生成的随机值 4bytes

固件应答认证命令

Byte offset	描述	取值
0	CMD	0xFF
1	ACK_CMD	应答的命令 CMD
2	ACK_TAG	应答命令的 SN
3	length	0x08，Payload 的长度
4~12	Payload	FW_Hash_new，固件生成新 hash 值的后 8byte

FW_Hash2

---生成方式，见广播包用户自定义数据说明。

FW_Hash_new

---使用 16byte 的 USER_DATA + 固件（MAC + APP_Random）共 28 个 bytes 的数据作为加密接口输入明文，固件的 FW_ramdom（广播包的随机值）数据作为输入 key，调用算法加密后会输出 16 个 byte 加密数据，然后抽取其中后 8 个 byte 作为 FW_Hash_new 应答给 APP 认证使用。

1.6 控制设备协议

建立连接后，APP 发送命令控制云台转动和 LED 亮灭灯。

APP 使用 UUID ab01 的 WRITE 属性向固件发送控制。由于蓝牙 ATT 协议有 WIRET RESPONE 的应答，所以暂定控制命令不需要固件应答，便于固件响应及时。

APP 发送控制命令

Byte offset	描述	取值
0	CMD	0x20
1	TAG	SN，不需要应答
2	length	0x02
3	Payload1	云台动作： 0x00--保持当前状态，不操作 0x01--顺时针转动 0x02--逆时针转动 0x03--停止转动 其他值未定义处理
4	Payload2	8 个 LED 状态，每 1bit 代表灯亮灭状态 1-亮。0-灭

1.7 连接控制

（1）设备未连接时 BLE 广播时间为 100ms。

（2）APP 打开时，通过 BLE 快速连接设备（不使用配对绑定方式）；APP 关闭则断开 BLE 连接。

（3）建立连接后，固件不主动调整蓝牙连接参数；统一由 APP 调整蓝牙通信的间隔参数，固定通信周期为 45ms，参数如下：

Connection_Interval_Min = 45 ms

Connection_Interval_Max = 45 ms

Connection_Latency = 0

Supervision_Timeout = 5000ms

（4）APP 通过命令来控制云台转动的距离以金 LED 灯亮灭的时间。

暂定 LED 灯亮灭的时间为 450 ms

1.8 加密模块

使用杰理自定义的加密模块 bt_hash_enc.a，基于 AES 模式设计实现的，手机 APP 和固件一致使用该加密方式加密数据。

固件接口如下：

```
/*
@param [in]    pt[*1]        The plaintext
@param ptlen                 The length of the plaintext(octets)          range: 1~32
@param [in]    key[*1]       The key for encrypt
@param keylen[*1]            The length of the key(octets)                range: 1~32
@param [out] mac[*1]         output : The Message Authentication Code     16 bytes.
*/
void btcon_hash(unsigned char *pt, int ptlen, unsigned char *key, int keylen, unsigned char *mac);
```