|  |
| --- |
| **JL爱拍协议** |
| **V0.05** |

This translated version is for reference only, and the English version shall prevail in case of any discrepancy between the translated and English versions.

版权所有 2020杰理科技有限公司未经许可，禁止转载

目录

[Chapter 1 JL爱拍协议 4](#_Toc6741)

[1.1概述 4](#_Toc1795)

[1.2广播包用户自定义数据 5](#_Toc6021)

[1.3 GATT 服务定义 6](#_Toc20047)

[1.4 通信协议格式 7](#_Toc27949)

[1.5 连接认证流程 8](#_Toc4687)

[1.6 控制设备协议 9](#_Toc31591)

[1.7 连接控制 10](#_Toc23960)

[1.8 加密模块 11](#_Toc10698)

**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 | |
| 0.0.3 | 2020/ 09/ 27 |  |
| 更新: | * 增加速度调节 | |
| 0.0.4 | 2020/ 10/ 09 | |
| 更新: | * 修改加密部分字节偏移描述错误 | |
| 0.0.5 | 2020/10/20 | |
| 更新: | * 增加对电机控制指令的说明 | |

# 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 |
| 8~13 | 6 | ble的mac地址低位先填入 |
| 14~17 | 4 | 随机数FW\_random，每次打开广播重新生成 |
| 18~25 | 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 2~13的数据）共28个bytes，作为加密接口输入明文，offset 14~17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 |  |

1. 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26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 | 0x03 |
| 3 | Payload1 | 云台动作：  0x00--不改变电机运动方向和速度  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 | 用来控制速度, 速度值范围是:0,1,2....10; 分别对应速度:0%, 10%, 20%......100%; (当Payload1=0时, 速度值无效 ) |
| 5 | Payload3 | 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);