# 车位锁4G通信协议

传输方式：UDP协议，数据都为JSON格式

服务器地址：域名方式，URL

基本信息：

|  |  |
| --- | --- |
| sn | 设备识别码 |
| cmd | 命令号 |
| version | 设备版本号 |
| nonce | 随机数 |
| sign | 签名方法，AES128，sn和nonce拼接，为32位 |
| result | 应答值 |
| status | 设备状态 |

1. 心跳

发送方：车位锁

{

"sn": "123456789", //设备编号，字符串，9字节

"cmd": 1, //命令号，0～255

"version" : 1, //固件版本编号，0～255

"nonce":"43276876", //随机数

"sign":"xxxxxxxxx" //签名：对sn、cmd、nonce进行AES128加密签名

}

应答方：服务器

{

"sn": "123456789",

"cmd": 1,

"result" : 0, //0=成功

"nonce":"43276876",

"sign":"xxxxxxxxx"

}

1. 遥控开

发送方：服务器

{

"sn": "123456789",

"cmd": 2,

"nonce":"43276876",

"sign":"xxxxxxxxx"

}

应答方：车位锁

{

"sn": "123456789",

"cmd": 2,

"result" : 0, //0=成功，1=失败

"nonce":"43276876",

"sign":"xxxxxxxxx"

}

1. 查询状态

发送方：服务器

{

"sn": "123456789",

"cmd": 3,

"nonce":"43276876",

"sign":"xxxxxxxxx"

}

应答方：车位锁

{

"sn": "123456789",

"cmd": 3,

"result" : 0, //0=成功，1=失败

"status" : 0, //0=未知，1=关，2=开（无车），3=开（有车）

"nonce":"43276876",

"sign":"xxxxxxxxx"

}

签名具体说明

1. 使用AES128算法，CBC模式，密钥（16字节）为

{0x59,0xDC,0x27,0x7F,0x08,0x3A,0x95,0x01,0xA4,0xBF,0x17,0x45,0xA5,0x69,0xE6,0x31}。

（2）使用sn和nonce数据拼接明文（16字节），sn取9字节，cmd取1字节，nonce取4字节，前面14字节计算CRC作为最后2字节。

（3）Sign为计算后的密文。

（4）例如：

{

"sn": "123456789",

"cmd": 2,

"nonce":"43276876",

"sign":"902D110A18FF69472C7820A4BAAA6092"

}

拼接sn&cmd&nonce = 0x3132333435363738390243276876

CRC（3132333435363738390243276876） = A080

明文 = 3132333435363738390243276876A080

密文 =