2.4G无线通信模组网络传输协议

# 协议简介

本协议应用于智城云2.4G无线通信模组间网络创建和通信，协议主要描述了模组无线网络通信用使用的数据格式及对应的数据内容和用途。对网络通信的加密及业务逻辑、网络组成方式等内容进行了解释，以便于开发者快速理解和应用该协议进行软件开发工作。

# 网络结构

无线通信协议中网络传输分为三层，分别为应用层、网络层、物理层。

**物理层：**实现射频芯片硬件驱动、数据传输、地址过滤、信道切换及通信质量的控制等

**网络层：**实现网络协议的解析、事件的处理和发送、部分业务逻辑的处理

**应用层：**用户层网络数据的管理、网络配置处理等

无线模组网络传输分层模型：

# 协议格式

无线通信协议根据不同层次进行相对应的划分

## 物理层数据格式

物理层数据是数据通信的基础，对数据的基本格式进行了规定，约定了网络节点之间的数据通信方式，数据格式如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 引导码 | 休眠模式 | 帧类型 | 地址信息 | 包序号 | 数据长度 | 数据内容 | 校验值 |
| 1B | 1bit | 7bit | 8B | 1B | 1B | - | 1B |

**引导码：**0xA5，固定引导码

**休眠模式：**发送方是否休眠设备（0：不休眠，1：休眠），仅组网帧该位无效。向休眠设备发送信息会先缓存起来，等休眠设备唤醒时（主动上报），再将缓存的数据发送给该设备。休眠设备的心跳时间要比非休眠设备的间隔时间长，故判断其上下线的时间也会更长。

**帧类型：**

* + 0：业务帧
  + 1：组网帧
  + 2：应答帧
  + 3：心跳帧

**地址信息：**

组网帧与其他两个类型的帧地址信息有所不同，由于组网时从模组未分配网络地址，故组网帧通信时使用MAC地址来确定数据的流向。业务帧和应答帧均使用组网后的“网段地址+网络地址”的方式进行通信。

**组网帧：**

|  |  |
| --- | --- |
| 目的MAC地址 | 源MAC地址 |
| 4B | 4B |

目的MAC地址指数据接收方的MAC地址，源MAC地址为数据发送方的MAC地址。

目的MAC地址全为FF时为广播包，否则为单播包

**业务帧、应答帧：**

|  |  |  |  |
| --- | --- | --- | --- |
| 段地址 | 目的地址 | 源地址 | 保留 |
| 4B | 1B | 1B | 2B |

段地址为组网后确定的网段的地址，一般为主模组的MAC地址

目的地址为数据接收方的网络地址（组网时分配），源地址为数据发送方的网络地址

若目的地址为FF，则表明为广播包，否则为单播包，另外主模组的网络地址始终为0

**包序号：**

用于标示数据包的序号，每条递增

**数据长度：**

数据内容的长度

**数据内容：**

网络层数据内容，详见[网络层数据格式](#_网络层数据格式)

**校验值：**

对校验位之前的全部数据进行校验和的值

另，大于一个字节的数值均使用**大端**格式表示

## 网络层数据格式

网络层数据对所有业务方面的数据内容进行了规定和解释

网络数据格式相对较为简单，分为类型和内容两部分：

|  |  |
| --- | --- |
| 网络类型 | 网络数据内容 |
| 1B | - |

**网络类型：**

* + 0x01：搜索网络
  + 0x02：设备信息
  + 0x03：添加设备
  + 0x04：删除设备
  + 0x05：协调通信
  + 0x06：用户数据

网络类型及数据内容详见[网络层协议内容](#_网络层协议内容)

# 安全策略

通信协议中发送的网络层的数据均通过AES算法进行加密处理，接收方需要通过秘钥进行解密来还原原始的数据。秘钥是通过主模组的MAC、从模组的MAC和组网时分配的随机数组成。

**AES加密秘钥规则：**

|  |  |  |  |
| --- | --- | --- | --- |
| 主MAC | 从MAC | 填充1 | 填充2 |
| 4B | 4B | 4B | 4B |

填充1、2内容是组网时由主模组分配的随机数填充而成，填充1为随机数进行填充的值，填充2为随机数的反码进行填充得到的值。例如：随机数为0x0A，则填充1的内容为0x0A、0x0A、0x0A、0x0A，填充2的内容为：0xF5、0xF5、0xF5、0xF5。

**组网帧与广播帧不进行加密处理**

# 网络层协议内容

## 搜索网络

数据类型：0x01

功能：

组网时主模组通过该消息可以搜索到处于待组网状态下的从模组信息，发送时需要携带主设备的设备类型。

数据内容：

|  |
| --- |
| 设备类型 |
| 6B |

设备类型参考《2.4G无线通信串口使用协议》中的介绍

## 设备信息

数据类型：0x02

功能：

处于组网状态的从模组收到搜索网络的消息后，需要上报给主模组自身的设备信息，包含设备类型和是否休眠。

数据内容：

|  |  |
| --- | --- |
| 设备类型 | 休眠模式 |
| 6B | 1B |

休眠模式：1=休眠， 0=不休眠

## 添加设备

数据类型：0x03

功能：

主模组将搜索到的从模组添加到网络时，发送给从模组该消息，同时告知该模组的网络地址、通信信道、加密随机数和发送心跳的时间信息。

数据内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络地址 | 通信通道 | 加密随机数 | 心跳时间 | 主设备类型 |
| 1B | 1B | 1B | 2B | 6B |

## 删除设备

数据类型：0x04

功能：

主模组将从模组从现有的网络中删除，删除后从模组将无法在网络中进行通信，收发数据。

数据内容：

内容为空

## 协调通信

数据类型：0x05

功能：

主模组协助两个从模组之间建立或解除数据通信关系。

数据内容：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 建立/解除 | 对方网络地址 | 对方MAC地址 | 设备类型 | 是否休眠 | 加密随机数 |
| 1B | 1B | 4B | 6B | 1B | 1B |

建立/解除：1=建立，0=解除

## 用户数据

数据类型：0x06

功能：

用户自定义的通信数据内容

数据内容：

用户自定义