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）。向休眠设备发送业务帧时会先缓存起来，等休眠设备唤醒时（接收到心跳或业务帧时），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（用户数据、协调通信、删除设备）
  + 1：组网帧（搜索网络、设备信息、添加设备）
  + 2：应答帧（用于对发送方业务帧的应答，表明已经到达接收方）
  + 3：心跳帧（用于维护主从设备之间的在线状态）

**地址信息：**

组网帧与其他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，组网帧通信时使用MAC地址来确定数据的流向。业务、应答和心跳帧均使用组网后的“网段地址+网络地址”的方式进行通信。

**组网帧地址信息：**

|  |  |
| --- | --- |
| 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。

**其他帧地址信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| 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，网段地址为主模组的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。保留2个字节留作以后扩展使用，暂不做处理。

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

## 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

为了保障用户的数据安全，业务帧的数据内容均先进行加密处理然后再发送。主模组在添加从模组时都会随机生成一个8位的加密Key，并通过添加设备消息将该加密Key发送给从模组，该Key将成为以后业务帧通信的加密秘钥，组网成功后，主从双方通信的业务帧数据内容都通过加密Key进行加解密操作。具体加密方式为将需要加密的数据按字节与加密Key进行异或操作，解密也是采用同样的操作方式。

另外，组网、应答、心跳帧与广播帧不进行加解密处理。

# 组网流程

组网是无线网络搭建最重要的一部分，模组之间建立通信的基础就是组网。

由于本协议为星形网络拓扑结构，所以每个网络中有且仅有一个主模组，主模组在网络中起到搜索、添加设备和分配网络地址的作用。

组网流程：

1. 主从模组均工作在组网的无线信道中
2. 主模组发送搜索网络的消息，该消息为广播
3. 接收到搜索消息的从模组，也通过广播上报本模组对应的设备信息
4. 主模组收到从模组的信息后会通知设备，然后根据设备的选择的信息发送添加设备消息，添加从模组进入网络中。添加设备消息中会包含从模组的网络地址、加密密钥、工作通信信道及从设备发送心跳的起始时间等。其中网络地址是和从设备的Mac地址一一对应的，所以要保证每个模组的Mac地址唯一性。每个设备的加密密钥是随机生成的，只有通信双发才能获取到该密钥。从模组的心跳起始时间是由主模组分配，为防止从模组间心跳冲突，从模组的心跳起始时间不会相同。
5. 添加完成后，从模组切换至工作信道中，等到心跳时间时，从模组发送心跳给主模组，主模组收到心跳后判断从模组上线，绑定成功。
6. 由于内部资源的限制，目前最大允许同时绑定5个从模组。

# 应答与重发机制

网络通信中为保证通信质量，网络协议支持重发机制，业务帧中除了广播包以外的所有通信消息接收方都需要进行应答处理，若超过200ms无应答，发送方将重发该消息，直到接收到接收方的应答消息为止（最大重发次数为3次）。

应答帧、心跳帧及广播帧不做应答重发处理。

# 上下线状态

主模组会定时维护从模组的在线的状态，并提供在线设备查询和上下线通知。当组网完成后从模组会定时（休眠设备为5分钟，非休眠设备为10秒一次）发送心跳给主模组消息，主模组收到后回复同样的心跳给从模组。当主从模组收到心跳后更新彼此的在线时间，当超过三次心跳时间没有接收到对方的心跳或则用户数据，则判定为对方离线。离线后当再次接收到对方的心跳或用户数据时，则重新判定为对方上线并更新在线时间。

# 协调通信

协调通信是基于星形网络基础上增加的功能，由于星形网络的通信方向仅为主从模组之间，从设备之间是无法直接建立通信的。协调通信功能主要是对从设备之间直接通信进行了拓展，主模组通过发送协调通信的消息，使两个从设备之间建立通信关系，当两个从设备接收到协调通信消息之后，就可以利用协调通信消息的信息和彼此进行直接通信了。协调通信消息内容包括对方的网络地址、加密密钥、设备类型等信息。

# 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。组网前由于不可能知道从模组的Mac信息，故该消息通过广播包发送。

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