产品应用笔记

ZigBee节点快速加入指定协调器

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.

目录

Zigbee节点快速加入指定协调器

1.Zigbee快速组网原理

传统Zigbee组网需要以下几个步骤：

① 协调器打开允许入网，并广播通知全部路由器也打开允许入网。
② 入网节点扫描网络，寻找空间中哪些协调器或者路由器打开了允许入网，入网节点要在多个信道之间切换寻找协调器或者路由器。
③ 入网节点找到了打开允许入网的协调器或者路由器，向该协调器或者路由器发送关联请求。关联请求中包含入网节点的MAC地址。
④ 协调器或者路由器收到了入网节点的关联请求后，为入网节点分配一个16bit短地址，并把自己的PANID发送给入网节点。
⑤ 如果是协调器接收关联请求，就把当前的协调器网络密钥发给入网节点；如果是路由器收到了关联请求，路由器先向协调器报告新入网节点的短地址，MAC地址，然后协调器通过新入网节点的短地址向新入网节点发送网络密钥。

根据上述组网流程，Zigbee设备组网成功的关键条件是入网节点需要获取到协调器的PANID，信道，网络密钥，并且自己还需要有一个16bit短地址。同时还要保证入网节点的RAM和ROM中的状态是“已入网”。满足上述条件则可以满足Zigbee节点入网需求。

具体操作方式如下：

① Zigbee入网节点先加入到任意协调器网络（协调器甲）中。保证该Zigbee入网节点的RAM和ROM中记录状态是“已入网”，并且有协调器已经分配好的16bit短地址，PANID，信道，网络密钥。
② 已知协调器乙的PANID，信道，网络密钥。使用协调器乙的PANID，信道，网络密钥替换掉入网节点中保存的协调器甲的PANID，信道，网络密钥。

上述方法使入网节点绕开了协调器乙的验证，协调器乙可以通过路由算法找到入网节点。但是存在以下两个风险。

① 协调器乙未记录入网节点的MAC地址信息，协调器乙的上位机软件会收到入网节点的数据。
② 协调器乙不保存入网节点的信息，理论上该方法可以使协调器乙不存在入网节点数量限制。
③ 入网节点之前绑定了协调器甲的MAC地址（虚拟设备SN），同时周期上报状态也是发给协调器甲。突然切换到协调器乙后，需要删除绑定协调器甲的MAC地址，并绑定协调器乙的MAC地址。

2.指令操作

按照HEX指令中“本地配置命令”的格式，新增本地配置命令0x0F

命令码：0x1F
功能：查询或修改节点中保存的网络参数。

命令格式1——查询当前网络信息
输入命令：

字段	命令码	命令数据
内容	0x1F	空
字节数	1	0

反馈命令：

字段	命令码	命令数据						
内容	0x1F	状态	信道	PANID	短地址	扩展PANID	网络密钥	密钥序号
字节数	1	1	1	2	2	8	16	1

示例
输入命令：55 03 00 1F 1F
返回命令：55 22 00 1F [00] [0F] [19 ED] [BD 71] [BD AB FA 0F 26 72 87 08] [14 BC D1 83 64 67 B9 C2 BA BD EA E0 95 19 2B 9A] [00] A2
返回命令解析：

状态：00，节点已入网
信道：0F，信道15信道
PANID：19 ED，PANID为0xED19
短地址：BD 71，短地址为0x71BD
扩展PANID：BD AB FA 0F 26 72 87 08
网络密钥：14 BC D1 83 64 67 B9 C2 BA BD EA E0 95 19 2B 9A
密钥序号：00

命令格式2——修改当前网络信息
输入命令：

字段	命令码	命令数据						
内容	0x1F	操作	信道	PANID	短地址	扩展PANID	网络密钥	密钥序号
字节数	1	1	1	2	2	8	16	1

反馈命令：

字段	命令码	命令数据
内容	0x1F	状态
字节数	1	1

示例：
输入命令：55 22 00 1F [01] [0F] [19 ED] [BA 57] [BD AB FA 0F 26 72 87 08] [14 BC D1 83 64 67 B9 C2 BA BD EA E0 95 19 2B 9A] [00] 82
返回命令：55 04 00 1F 00 1F

操作：01，节点已入网
信道：0F，信道15信道
PANID：19 ED，PANID为0xED19
短地址：BD 71，短地址为0x71BD
扩展PANID：BD AB FA 0F 26 72 87 08
网络密钥：14 BC D1 83 64 67 B9 C2 BA BD EA E0 95 19 2B 9A

3.注意事项

① E180-ZG120系列模组，切换协调器后需要复位才生效。
② E18系列模组作为路由器使用时，可以不用复位，但是最好是复位一下。
③ E18系列模组作为终端节点或者休眠节点，在发送0x1F命令修改网络配置后，需要立即复位。
④ E18系列模组作为终端节点或者休眠节点，在当前网络无协调器和路由器的情况下会周期性的尝试重连原协调器或者路由器，修改组网信息命令应该在两次重连之间进行操作（以异步命令“网络状态变更”且网络状态值等于0x03为准），两次重连间隔时间10秒，务必在这10秒内完成修改命令的下发和模组复位（命令复位或者外部引脚复位都可以）。

关于我们

销售热线：4000-330-990 技术支持：support@cdebyte.com
官方网站：www.ebyte.com
公司地址：四川省成都市高新西区西区大道199号B5栋

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.