

基于 ZigBee 无线传感器网络的通信标识管理终端通信研究

李秉毅¹ 梁柯¹ 胡音² 邓雪波¹ 温永怡¹

(国网重庆市电力公司 重庆 400017)¹ (国网重庆垫江县供电有限责任公司 重庆 408300)²

摘要 首先介绍了无线传感器网络和 ZigBee 技术的相关基础知识,然后在现有的 ZigBee 硬件方案中选择了 Freescale 公司提供的解决方案,MC13224。接着在深入分析 ZigBee 协议规范的基础上,对 ZigBee 协议的网络层、应用层作了介绍。最后,介绍了基于通信标识管理终端对 ZigBee 网络的组网进行测试的方法。

关键词 无线传感器网络, ZigBee, MC13224

中图分类号 TP393.02 文献标识码 A

Communication Research of Communication Identity Management Terminal Based on ZigBee Wireless Sensor Networks

LI Bing-yi¹ LIANG Ke¹ HU Yin² DENG Xue-bo¹ WEN Yong-yi¹

(Chongqing Electric Power Company, State Grid, Chongqing 400017, China)¹

(Chongqing's dianjiang County Limited Liability Company, State Grid, Chongqing 408300, China)²

Abstract This paper firstly introduced the related knowledge about the wireless sensor network and ZigBee technology, and then choosed a ZigBee hardware scheme offered by Freescale, named MC13224. After reading and analyzing the ZigBee protocol, this paper described the NWK layers and application layer. Then we developed a simple application instance on this platform. After that data structures and important functions to implement the application were discussed. Finally this paper showed the application by a third party software, and introduced the method of testing the ZigBee net working mode based on the communication terminal identification management.

Keywords Wireless sensor network, ZigBee, MC13224

无线传感器网络综合了传感器技术、无线通讯技术和计算机技术等,具有信息采集、传输和处理的能力。低成本、低功耗、应用简单的 ZigBee 协议的诞生为无线传感器网络及大量基于微控制的应用提供了互联互通的国际标准。

本应用基于 MC13224 平台进行了二次开发,在成功组建 ZigBee 网络的基础上实现了读取传感器参数、控制 LED 灯等功能,并且节点可以根据光线的强弱自动控制 LED 灯的开关,以模拟对特定家居的控制。结果表明该应用软件实现了基于 ZigBee 网络的传感器检测与控制。

1 ZigBee 技术简介

1.1 ZigBee 技术特征

ZigBee 的技术特征如表 1 所列。

表 1 ZigBee 的技术特征

指标	值
工作频段	2.4GHz, 868MHz, 915MHz
最高数据传输速率/kbps	250, 20, 40
覆盖范围/m	10~100
协议栈容量/KB	28
功耗	极低
模块成本/美元	2
可连接的设备数量	254
响应速率	极快

ZigBee 技术是一种短距离、低复杂度、低功耗、低数据速率、低成本的双向无线通信技术或无线网络技术,是一组基于 IEEE 802.15.4 无线标准研制开发的有关组网、安全和应用软件方面的通信技术。ZigBee 是这种技术的商业化命名。

1.2 ZigBee 协议栈概述

ZigBee 协议栈由一组子层构成。每层为其上层提供一组特定的服务,一个数据实体提供数据传输服务,一个管理实体提供全部其它服务。每个服务实体通过一个服务接入点(SAP)为其上层提供服务接口,并且每个 SAP 提供了一系列的基本服务指令来完成相应的功能。

ZigBee 协议栈的体系结构如图 1 所示。

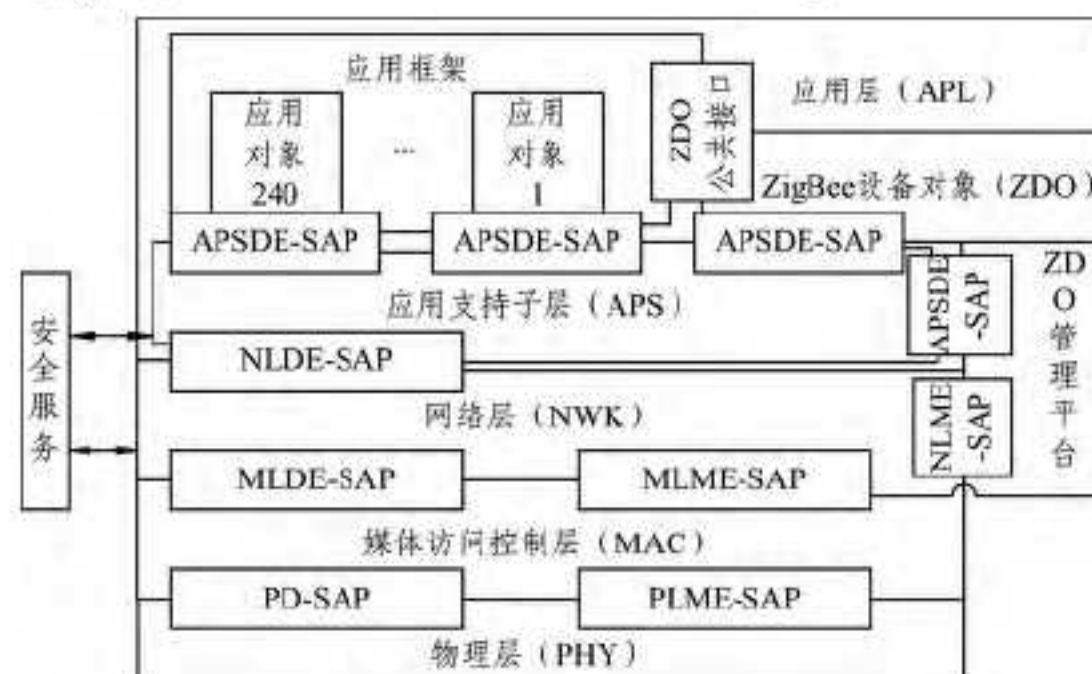


图 1 ZigBee 协议栈的结构

李秉毅(1981—),男,硕士,工程师,主要研究方向为电力通信;梁柯(1979—),男,硕士,工程师,主要研究方向为电力通信;胡音(1975—),女,工程师,主要研究方向为电力通信;邓雪波(1975—),男,硕士,高级工程师,主要研究方向为电力通信;温永怡(1963—),女,硕士,高级工程师,主要研究方向为电力通信。

1.3 ZigBee 网络层协议规范

网络层管理实体提供网络管理服务,允许应用与协议栈相互作用。网络层管理实体应该提供的服务包括:配置一个新的设备,为保证设备正常工作的需要,设备应具有足够资源,以满足配置的需要,配置选项包括对一个 ZigBee 协调者和所连接的一个现有网络设备的初始化操作,初始化一个网络,使之具有建立一个新网络的能力,连接和断开网络,具有连接或者断开一个网络的能力,以及为建立一个 ZigBee 协调者或者 ZigBee 路由器,具有要求设备同网络断开的的能力;ZigBee 协调者和 ZigBee 路由器具有为新加入网络的设备分配地址的能力,邻居设备发现,具有发现、记录和汇报有关邻居设备路由的能力,路由发现,具有发现和记录有效地传送信息的网络路由的能力,接收控制,具有控制设备接收机接收状态的能力,即控制接收机什么时间接收、接收时间的长短,以保证 MAC 层的同步或者正常接收等。

1.4 ZigBee 应用层规范

ZigBee 应用层由 3 个部分组成:应用支持子层、应用层框架和 ZigBee 应用对象(ZDO)。

应用支持子层给网络层和应用层通过 ZigBee 设备对象和制造商定义的应用对象使用的一组服务提供了接口,该接口提供了 ZigBee 设备对象和制造商定义的应用对象使用的一组服务。通过两个实体提供这些服务:数据服务和管理服务。应用支持子层数据实体(APSDE)通过与之连接的服务接入点,即 APSDE-SAP 提供数据传输服务。应用支持子层管理实体(APSME)通过与之连接的服务接入点,即 APSME-SAP 提供管理服务,并且维护一个管理实体数据库,即应用支持子层信息库。

ZigBee 中的应用框架是为驻扎在 ZigBee 设备中的应用对象提供活动的环境。最多可以定义 240 个相对独立的应用程序对象,任何一个对象的端点编号从 1 到 240。还有两个附加的终端节点为 APSDE-SAP 的使用,端点号 0 固定用于 ZDO 数据接口,另外一个端点 255 固定用于所有应用对象广播数据的数据接口。端点 241—254 保留(用于扩展使用)。

ZigBee 设备对象(ZDO)描述了一个基本的功能函数,这个功能在应用对象、设备 profile 和 APS 之间提供了一个接口。ZDO 位于应用框架和应用支持子层之间。它满足所有在 ZigBee 协议栈中应用操作的一般需要。

2 标识管理终端通信

通信标识是通信基础资料尤其是现场设备和配线资料的重要组成部分,对指导现场工作人员安全作业起到了重要作用。通信标识的准确性,以及现场资料与运维资料的一致性举足轻重,是顺利开展通信网络运行维护工作的基础。

在国内,信息产业部于 2000 年组织制定了《建筑与建筑群综合布线工程系统设计规范》和《建筑与建筑群综合布线系统工程验收规范》。但是,这两个规范对于标识管理在建筑与建筑群综合布线工程系统中的作用和地位的认识是不足的。两个规范与美国标准、国际标准比较是严重滞后工程实际的,规范的先进性也是不足的。迄今,我国信息产业没有对标识提出标准。

重庆市电力公司于 2013 年 9 月制定了通信标识资源管理办法,对通信资源的权责界面进行了划分,对通信设备的标

识方法及标识规范进行了定义。为了配合通信标识管理办法的实施,需要利用信息化手段提供有力的技术支持。其中,标识管理终端的设计极为重要。

标识管理终端采用手持式嵌入式终端设计,需要提供 RFID 读写、一维码和二维码扫描识别等功能。

出于安全性考虑,标识管理终端的无线数据传输要求采用非 WIFI 方式,同时要兼顾小自组网的要求。因此,考虑采用 ZigBee 网络作为通信标识终端通信手段之一,作为特殊场景下的补充通信手段。在较小范围之内采用星型组网或者点对点组网进行实时通信,在较大范围内采用多级中继方式实现终端实时通信功能,以保证特殊场景下的应急通信功能。

3 ZigBee 无线网络组网

3.1 EXPLORERF-MC13224 无线传感器平台

本平台以 FreeScale 公司的以 ARM7 为内核的 ZigBee 芯片 MC13224 为核心,该芯片支持国际 802.15.4 标准以及 ZigBee、ZigBee PRO 和 ZigBee RF4CE 标准,提供了 104dB 的链路质量、优秀的接收器灵敏度和健壮的抗干扰性、多种供电模式、多种传感器,以及一套广泛的外设集,包括 2 个高速 UART、12 位 ADC 和 64 个通用 GPIO、4 个定时器、I2C 等。

EXPLORERF-MC13224 是 MC13224 的升级版,完全满足 IEEE 802.15.4 标准和 ZigBee2007/PRO 技术标准的无线网络技术开发,如图 2 所示。

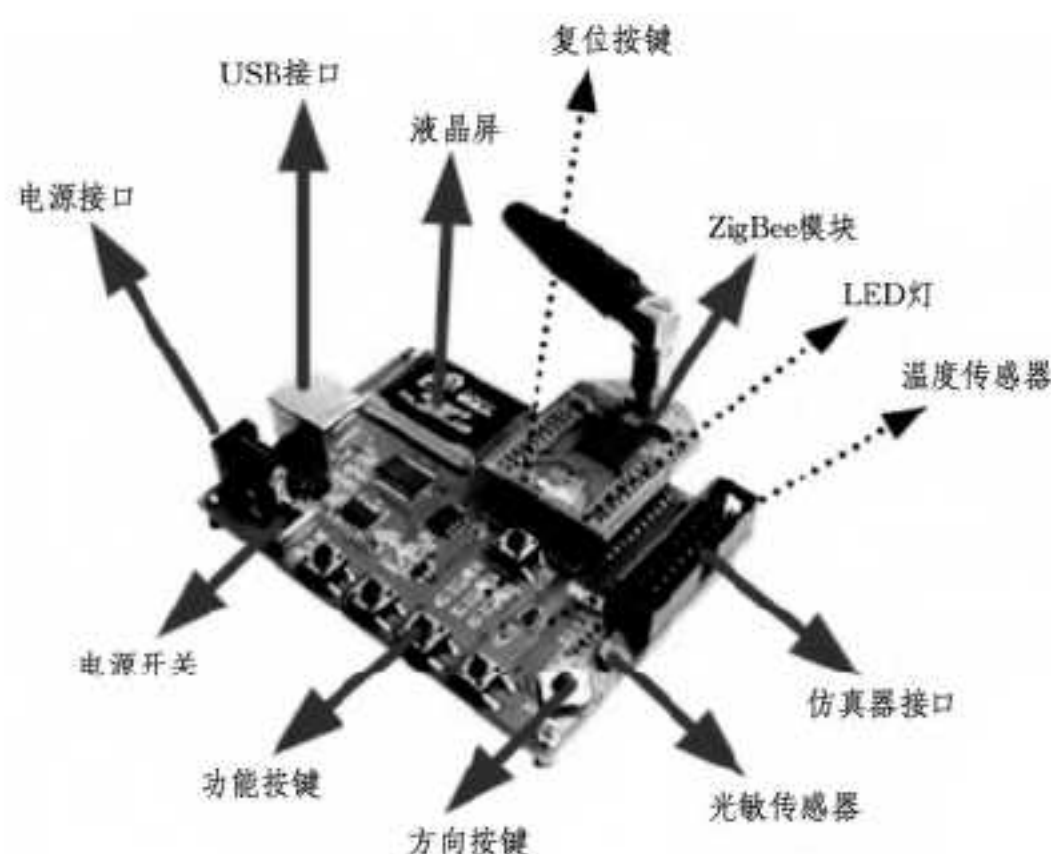


图 2 EXPLORERF-MC13224 网关

其工作流程是:当计算机发送命令以后,网关接收命令,首先判断是不是可用的命令,如果可用,根据命令判断计算机需要哪个节点的信息,并向该节点发送命令要求将对应数据传回网关,然后再将接收到的指定节点的信息按既定格式发送给 PC 机,PC 机通过传感器网络 PC 软件显示出来。

3.2 BeeStack 协议栈

对于 MC1322x 来说,FreeScale 公司提供了 BeeStack 协议栈,可以生成不同应用模板。BeeStack 协议栈为非抢占式轮转查询式操作系统,已经编写了从 MAC 层(macEventLoop)到(ZDapp-event-loop)五层任务的事件处理函数。开发者一般情况下只需要编写应用层的任务和处理函数即可。

3.3 ZigBee 网络组网设计

EXPLORERF-MC13224 无线传感器平台内配置了 ZigBee2007/PRO 协议栈,在没有进行网络拓补修改之前支持 5 级路由,31101 个网络节点。传感器网络结构图如图 3 所示。



图3 ZigBee网络拓扑设计

EXPLORERF-MC13224 无线传感器平台由 PC 机部分、网关部分、网络节点部分组成。列出每部分的主要功能如下:

①PC 机:接收网关数据和发送指令,实现可视化、形象化人机界面,方便用户操作、观察。

②网关:完成通过计算机发送的指令,发送或接收路由节点或者传感器节点的数据,并将接收到的数据发送给计算机。

③网络节点:网络节点包括两大功能:1)在网关不能和所有的传感器节点通信时,路由节点作为一种中介使网关和传感器节点通信,实现路由通信功能;2)控制设备和采集数据,包括对 LED 灯的控制,采集温度、光照度数据等。

4 ZigBee 无线传感器网络应用

4.1 ZigBee 网络协调器的软件实现

采用星状网络拓扑搭建无线局域网。星状网是以网络协调器为网络中心,网络协调器不仅负责数据的传送,而且负责整个网络的形成和管理,是整个网络的大脑。网络协调器应用层的重要步骤如下:

①定义端点与设备。每个应用对象通过一个端点连接到 ZigBee 协议栈的余下部分,因此从应用角度看,通信的本质就是端点到端点的连接。

②定义输入簇 ID 数组与输出簇 ID 数组。端点之间的通信是通过簇来实现的,这些簇是应用对象之间共享信息所需的全部属性的容器,在特殊应用中使用的簇在模板中有定义。

③创建绑定表。绑定创建端口之间或应用对象之间的逻辑连接,网络协调器为整个网络维护绑定表。

④无线信道的访问机制。采用的是非信标网络。因此信道的访问方式主要是非时隙的免冲突载波检测多路接入算法(CSMA/CA)。

⑤信道能量检测扫描。能量检测扫描使设备能检测到每个信道的能量峰值。

⑥信道能量检测结果的处理与信道选择。信道能量检测的结果记录在确认消息实体中,记录在能量检测值的列表中。

⑦开启网络协调器。首先程序把预先设定的网络协调器网络短地址通过 MAC 设置命令写入 MAC 层的参数属性库,接着程序同样通过 MAC 设置命令把网络协调器设置为允许节点接入。

⑧协调器对设备请求连接的处理。网络协调器把 macAssociationPermit 设置为 TRUE 时,协调器才允许其它节点设备进行连接。设备通过发送 MLME-ASSOCIATE.request 原语请求同一个已经存在的网络协调器进行连接。协调器正确接收到该请求后则发送一个确认帧给节点设备,表示成功接收请求。然后协调器在设定的时间内决定网络当前的资源是否足够允许另外一个设备的接入,如果协调器发现此设备之前已经连接到本 PAN 上,则将删除所有之前所获得的设备信息。

⑨非信标网络的同步。在不支持信标的 PAN 上工作的所有设备,根据上层的判断,轮询处理协调器的数据。MAC

层管理实体接收到 MLME-POLL.request 原语后,命令设备轮询协调器,MAC 层管理实体将按照从协调器提取未决数据的过程进行操作。

⑩协调器提取未决数据操作。在非信标网络中,协调器若要发送数据至节点设备,则协调器先将数据存储在协调器,然后加入未决事务列表。节点设备通过轮询发送数据请求命令至协调器。协调器一旦成功地接收数据请求命令,将发送确认帧来确认接收。

协调器程序流程如图 4 所示。

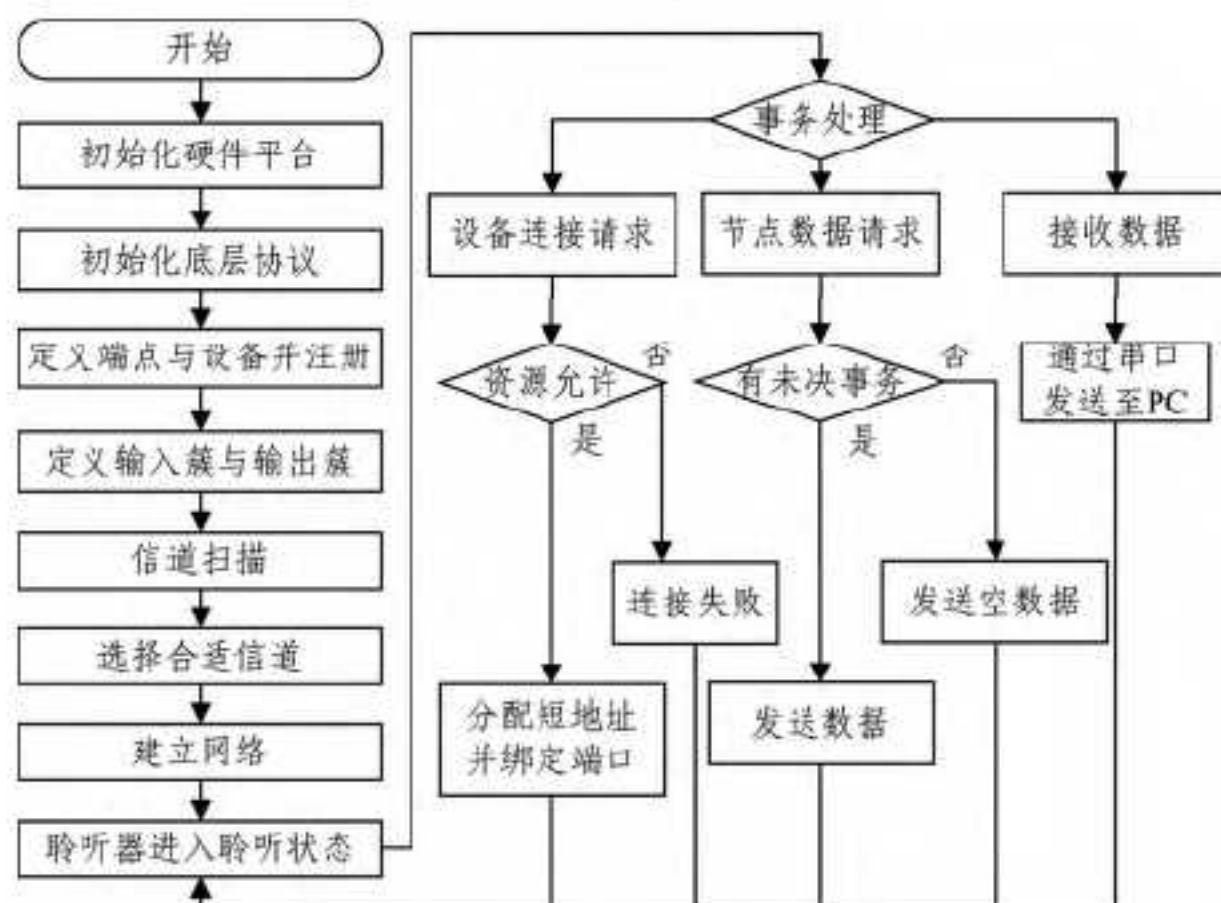


图4 协调器程序流程图

4.2 ZigBee 网络节点的软件实现

ZigBee 网络节点要实现的功能主要是加入现存的无线局域网,获取传感器的数据,然后与网络协调器相互通信。网络设备节点既是信息采集者也是控制信息的执行者。

网络节点程序流程如图 5 所示。

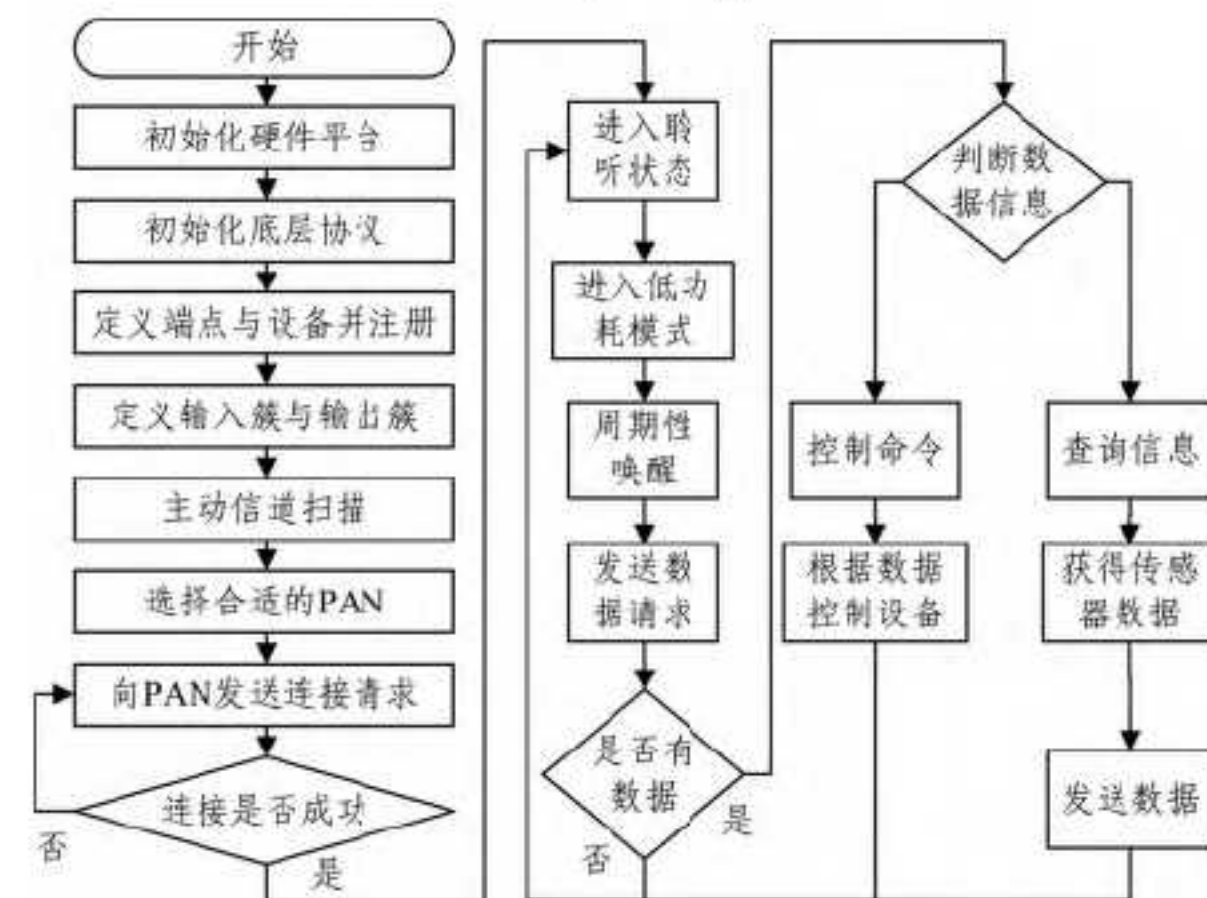


图5 网络节点程序流程图

主要流程包括:

①主动信道扫描。设备主动发送信标请求命令,对在其域工作范围内任何协调器发射的信标帧进行锁定,在设备接入网络之前,设备可以使用主动信道扫描,然后选择 PAN 标识符,最后加入选择的网络。主动扫描期间,MAC 层将丢弃所有物理层数据服务发来的非信标帧信息。

②主动信道扫描结果的处理。从 MAC 管理实体中接收到主动信道扫描的确认消息,提取消息中的 PAN 描述符列表,根据信息中的信标传输链路质量值的大小选择合适的局域网,选择信标传输链路质量值最大的 PAN 描述符,然后把选中的 PAN 描述符的信息存储入相应的属性库里,最后向

选中的 PAN 协调器发送连接请求

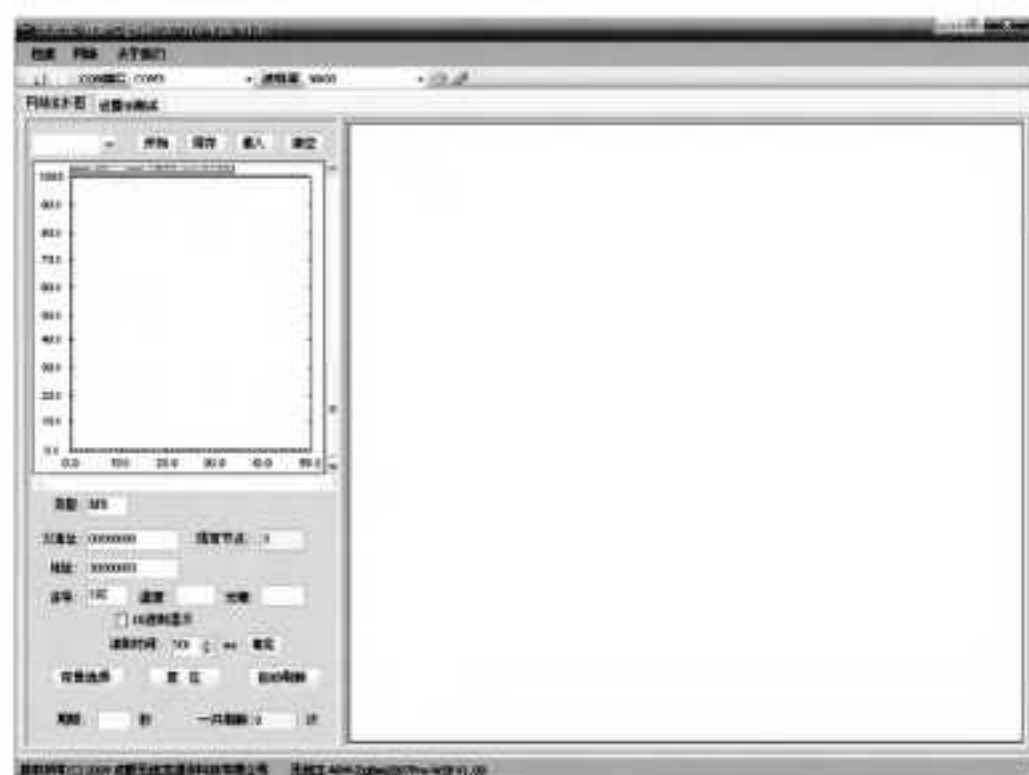
③间接传输方式。协调器发送数据至设备子节点采用的是间接传输方式,协调器首先把数据存储在缓冲区,然后等待设备子节点进行数据请求。

④上层数据控制协议。若子节点设备接收到来自协调器的数据的第₁个字节为0x01时,则表明数据的第₂个字节是用来控制子节点设备上的LED灯的显示状态。若子节点设备接收到来自协调器的数据的第₁个字节为0x02时,则表明协调器命令子节点发送当前LED灯的显示情况以及各个传感器的数据至协调器

5 通信标识管理终端 ZigBee 无线网络组网测试

5.1 网络监控软件

打开 ZigBee 无线传感器监控软件如图 6 所示。



分步连接网络与网络拓扑图

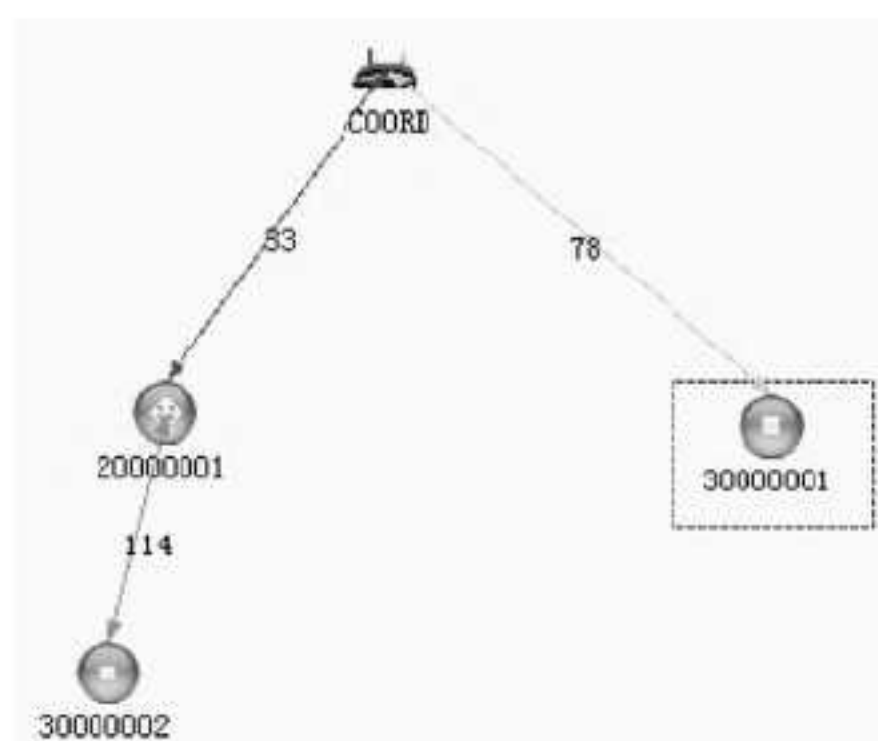
① 正解打开串口后,选择“网络拓扑图”,注意确保网关与计算机的正确连接。

②根据所设的周期自动刷新网络(注:自动刷新开启后不能执行其它与硬件交互的命令)。

③在打开自动刷新后,就可以开始组建网络了,首先将下载有路由器程序(如图 7 中地址为“20000001”的节点)的节点电源打开,打开电源后再按 S1 键并确定节点模块上闪烁的 LED 灯已停止闪烁,这样就表示已连入网络。

④现打开下载了终端节点程序的终端节点(地址为“30000002”的节点)的电源,通过路由器(地址为“20000001”的路由功能节点)加入网络

⑤ 在离网关不远处开启一个终端节点(地址为“30000001”),使该节点能直接通过网关接入网络。如图7所示,网络建立完毕。



5.2 手动设置测试

要转到“设置与测试”，只需单击“设置与测试”的标签

①先在节点树选择要设定的节点

② 选择命令发送方式

命令发送有两种方式。

1) 在下拉框中选择“命令头”方式发送

2) 直接在“输入命令文本框”里输入命令,命令格式为“命令头+帧数+数据”(注意,当“输入命令文本框”里有数据时,将“输入命令文本框”里的命令“优先”发送)。

表 2 RND(网络发现)命令表

描述	发现当前网关连接的网络
适用范围	网关
发送命令	&RND00000000000000000000000000000000* &RND+ 地址(10 字节)+ 返回网络中节点的性质
返回	(RFD(终端节点)/ROU(路由器))+ 第几个(2 字节)+000000000000* 发送:&RND00000000000000000000000000000000* 返回:&RND20000001 ?? ROU0000000000000000 ?*
例	&RND30000001 ?? RFD0100000000000000 ?* &RND30000002 ?? RFD0000000000000000 ?* &RND0000000000END0000000000000000 ?*

注：字符_x表示任意字符

表 3 RASWD(读温度传感器)命令表

描述	读取指定地址节点的温度
适用范围	RFD(终端节点)/ROU(路由器)
发送命令	&RAS+地址(10 字节)+WD+15 个 0+*
返回成功	&RAS+地址(10 字节)+WD+测量值(2 字节)+13 个 x+*
返回失败	&RAS+地址(10 字节)+E0+15 个 x+*
例	发送:&RAS30000001xxWD0000000000000000* 返回成功:&RAS30000001xxWD32xxxxxx xxxxxx*? 返回失败:&RAS30000001xxE0xxxx xxxxxx xxxxxx*?

注: RASGM 命令头; RASGM 表示当前节点的光敏感度

通过上述命令的发送,对接收到的数据进行观察,判断网络是否联通。

结束语 本文系统研究了 ZigBee 技术和 IEEE 802.15.4 标准,重点研究了 ZigBee 技术协议和组网技术,确定了 ZigBee 开发平台的结构框架。同时在此基础上进行了通信标识管理终端的 ZigBee 组网方式的测试验证工作,进一步验证了 ZigBee 的工作模式和通信协议规范。

参考文献

- [1] ZigBee 联盟. ZigBee 技术引领无线数字新生活[J]. 电脑知识与技术, 2006, 27: 29-34
- [2] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005
- [3] 孙亭, 杨永田, 李立宏. 无线传感器网络技术发展现状[J]. 电子技术应用, 2005, (6): 1-5
- [4] ZigBee Alliance. ZigBee Specification[R]. ZigBee Alliance, Inc, 2007
- [5] 蒋挺, 赵成林. 紫蜂技术及其应用[M]. 北京: 北京邮电大学出版社, 2006
- [6] 张宏锋, 李文锋, 等. 基于 ZigBee 技术的无线传感器网络的研究[J]. 武汉理工大学学报, 2006, 28(8): 12-15

(下转第 361 页)

SCST 中的数据在目标端和后端设备间都是零拷贝的,不需要额外的内核空间。

在实验过程中,iSCSI 客户端启动器使用的是 open-iscsi 2.0.873^[9],服务器端目标器使用的是 iSCSI Enterprise Target(iet)^[10],客户端和服务端都运行于 ubuntu13.04。USB Key 购于海泰方圆公司。

针对文中讨论的两种安全问题,分别在 Windows 系统和 Linux 系统中进行了测试。

1. 攻击者在获得了用户名和密码,但是没有用户 USB Key 的情况下,进行登录,如图 2 所示,结果显示登录失败。



图 2 Windows 中攻击者登录失败

2. 攻击者在获得了用户名和密码,合法用户正常登录的情况下,进行登录,结果显示登录失败,而合法用户的通信不受影响。

图 3 显示在用户输入正确的用户名和密码后,登录成功。此时,窃取了用户名和密码的攻击者在另一台电脑上进行登录,图 4 显示攻击者登录失败,合法用户的使用不受影响。

```
# iscsiadm -m discovery -t sendtargets -p 10.6.12.62:3260
10.6.12.62:3260,1 iqn.foo.example.chap.enhance
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.authmethod --value=CHAP# iscsi-
adm -m node -T iqn.foo.example.chap.enhance -o update --
name node.session.auth.username --value=lee
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.password --value=123456789011
# iscsiadm -m node -T iqn.foo.example.chap.enhance -p 10.6.
12.62:3260 -l
Logging in to [iface: default, target: iqn.foo.example.chap.enhance,
portal: 10.6.12.62:3260]
Login to [iface: default, target: iqn.foo.example.chap.enhance, por-
tal: 10.6.12.62:3260] successful.
```

图 3 Linux 中合法用户登录成功

```
# iscsiadm -m discovery -t sendtargets -p 10.6.12.62:3260
10.6.12.62:3260,1 iqn.foo.example.chap.enhance
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.authmethod --value=CHAP# iscsi-
adm -m node -T iqn.foo.example.chap.enhance -o update --
```

```
name node.session.auth.username --value=lee
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.password --value=123456789011
# iscsiadm -m node -T iqn.foo.example.chap.enhance -p 10.6.
12.62:3260 -l
Logging in to [iface: default, target: iqn.foo.example.chap.enhance,
portal: 10.6.12.62:3260]
iscsiadm: Could not login to [iface: default, target: iqn.foo.example.
chap.enhance,portal: 10.6.12.62:3260]:
iscsiadm: initiator reported error(19 - encountered non-retryable
iSCSI login failure)
```

图 4 攻击者使用相同用户名和密码登录失败

结束语 本文讨论了 iSCSI 协议中 CHAP 身份认证方法在使用中的不足,即密码易泄露和允许多点登录,提出了使用 USB Key 对 iSCSI 的身份验证过程进行加固,攻击者必须在同时获得用户密码、USB Key 以及 USB Key 的 PIN 码的情况下才能成功登录,因此大大提高了 iSCSI 身份认证的安全性和稳定性。

参考文献

- [1] Satran J, Meth K, Sapuntzakis C, et al. Internet Small Computer Systems Interface(iSCSI). IETF RFC 3720, 2004. [EB/OL]. <https://www.ietf.org/rfc/rfc3720.txt>
- [2] Simpson W. PPP Challenge Handshake Authentication Protocol. IETF RFC 1994, 1996. [EB/OL]. <https://www.ietf.org/rfc/rfc1994.txt>
- [3] Leduc G. Verification of two versions of the challenge handshake authentication protocol(CHAP)[J]. Annales des télécommunications. Springer-Verlag, 2000, 55(1/2): 20-30
- [4] 朱珂. iSCSI 存储系统中的安全性研究[D]. 上海: 上海交通大学, 2007
- [5] 刘明. 基于 iSCSI 协议的网络存储安全技术研究[D]. 郑州: 中国人民解放军信息工程大学, 2007
- [6] 陈龙辉. 移动 PKI 体系中 SD 安全模块的研究[D]. 北京: 北京邮电大学, 2008
- [7] Vishwakarma S, Bagaria S. iSCSI Simulation Study of Storage System[C] // Cambridge, UK, Computer Modeling and Simulation, 2008, 4: 703-707
- [8] Alaidaros H M, Rasid M F A, Othman M, et al. Enhancing Security Performance with Parallel Crypto Operations in SSL Bulk Data Transfer Phase[C] // Penang: Telecommunications and Malaysia International Conference on Communications, 2007, 5: 129-133
- [9] Aizman A, Yusupov D. Open-iSCSI[OL]. <http://www.open-iscsi.org/>
- [10] iSCSI target[OL]. <http://iscsitarget.sourceforge.net/>
- [7] Fukui K, Fukunaga S, Tanimoto K. ZigBee technology for low-cost and low-power radio communication systems[J]. Journal Institute of Electronics Information and Communication Engineers, 2005, 88(01): 40-45
- [8] 于海斌, 曾鹏, 等. 智能无线传感器网络系统[M]. 北京: 科学出版社, 2006
- [9] 金纯, 罗祖秋, 罗凤, 等. ZigBee 技术基础及案例分析[M]. 北京: 国防工业出版社, 2008
- [10] 李文仲, 段朝玉. ZigBee 无线网络技术入门与实践[M]. 北京: 北京航空航天大学出版社, 2007
- [11] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless Sensor Networks: A Survey[J]. IEEE Computer, 2002, 38(4): 393-422

(上接第 354 页)