基于 ZigBee 和 WiFi 的双模网关设计方案

基于 IEEE802.15.4 标准的 ZigBee 协议具有自组织、稳定性好、抗干扰性强、功耗低等优点，主要应用于农业、工业检测、军事和医疗等方面。但其控制中心多是 PC，不能适应野外等特殊环境。WiFi 作为一种越来越普及的无线通信技术，凭借覆盖范围广、无需布线等优点，广泛存在于人们的生产生活中。以此提出一种适应于复杂环境的双模无线网关设计方案，具有良好的应用性和前瞻性。

1 系统总体结构

系统由 ZigBee 模块、开发板模块和 WiFi 模块组成。ZigBee 模块中，Coordinator 作为 ZigBee 网络的中心节点，负责控制和监测 ZigBee 路由节点，每一个路由节点携带一个传感器，负责把传感器采集的数据发送给 Coordinator。开发板模块作为协议转换的枢纽，用于解析 Coordinator 传输的数据。WiFi 模块，将开发板解析的数据封装成 WiFi 帧。这样就实现双模无线网关的转换，系统结构如图 1 所示。

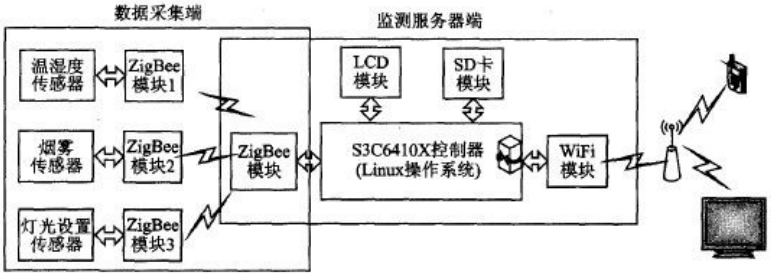

图 1 系统总体结构

2 无线网关的设计

2.1 ZigBee 数据流分析

ZB253002 模块是基于 CC2530F256 芯片，执行 ZigBee2007/PRO 协议的 ZigBee 模块，它具有 ZigBee 协议的全部特点。其主要的特点：

①自动组网。所有的模块通电即自动组网，协调器（Coordinator）自动给所有的节点分配地址，不需要用户手动分配地址，网络加入、应答等专业 ZigBee 组网流程。

②简单数据传输。ZB253002 模块可以理解为“无线的 RS232 连接”，通过串行端口即可在任意节点间进行数据传输。ZigBee 模块有两种数据的传输方式：数据透明传输，只要传送的第一个字节不是 0xFE、0xFD 或 0xFC，

则自动进入数据透明传输方式；点对点的数据传输方式，数据传输的格式为 0xFD（数据传输命令）+
0x0A（数据长度）+（目标地址）+（数据）。由协调节点传输给开发板的数据添加以 0xFE 开头的 15 字节的节点信息，用来提供给 TI Sensor Monitor，观察网络结构。

Zigbee 模块设置命令表如表 1 所列。

输　入	返　回	功　能
FC 02 91 01 XX XX	XX XX	设置模块的 PAN ID
FC 00 91 02	19 8B	恢复 PAN ID 为默认值，同时清除 FLASH 默认值
FC 00 91 03	XX XX	读取模块的 PAN ID
FC 00 91 04	XX XX	读取模块的网络地址
FC 00 91 05	XX XX	读取模块串口波特率
FC 01 91 06 *	XX XX	设置串口的波特率，* 为 01～05，代表 5 种波特率
FC 00 91 07	01 02 03 04 05	测试串口波特率

表 1 Zigbee 模块设置命令表

2.2 通信协调器的设计

Coordinator 是整个网关转换和无线传感器网络建立的中心，是数据传输的中心枢纽。因此，Coordinator 的设计关系到整个系统的稳定性和可靠性。Coordinator CC2530 采用 ZigBee2007 协议栈。ZStack 是 TI 公司提供的一种轮询式操作系统，借助于 Z-Stack，Coordinator 上电后，首先进行硬件和网络初始化，然后创建 3 个任务：①ZigBee 网络任务，该任务通过 Coordinator 与其子节点的“绑定”完成。其绑定的过程，协调器建立网络，创建绑定表，并设定允许绑定模式，子节点发送绑定请求，Coordinator 更新绑定表并响应子节点。②串口协议解析任务，该任务用于解析来自开发板和子节点的数据，并将解析后的数据传输给子节点任务或发送给开发板。③子节点任务，该任务主要用于接收子节点返回的数据，并将数据传输给串口协议解析任务。这样 ZigBee 协议帧的解析就转到开发板端，由 Linux 操作系统完成，Linux 解析完成后，将有效的数据放入指定的共享内存。当 BOA 收到外部 Web 请求，调用相应的 CGI 获取共享内存中的数据，并经由无线网卡以 WiFi 的形式传送给用户。

2.3 传输协议的实现

本设计经由 Linux 操作系统完成 ZigBee 协议的解析和 WiFi 协议帧的形成，主要的重点在于 Coordinator 与 Linux 串口传输协议的设计。串口传输协议自定义帧格式如下：

帧头	功能号	有效数据长度	有效数据	FCS 校验
8 位	16 位	8 位	可变	16 位

串口传输协议自定义帧格式

自定义帧的格式由帧头、功能号、有效数据长度、有效数据和 FCS 校验 5 部分组成。帧头定义为 0x02；功能号因获取的数据类型不同而异，有关帧格式功能码定义如表 2 所列；有效数据长度用于标识读取有效数据的长度范围，最大值为 255；有效数据存放 ZigBee 协议帧；FCS 校验用于数据段的校验。

标记值	宏定义	功能说明
0x5001	CMD_NET_CON_REQ	请求 ZigBee 网络连接状态
0x5002	CMD_NET_DESP_REQ	请求 ZigBee 网络基本信息
0x5003	CMD _ NET _ TOPO _ REQ	请求 ZigBee 网络拓扑信息
0x5004	CMD_GET_SENSOR_STATUS_REQ	请求获得传感器状态信息
0x5005	CMD_SET_SENSOR_STATUS_REQ	请求设置传感器状态
0x5006	CMD_SET_SENSOR_SLEEP_REQ	请求设置传感器休眠
0x5007	CMD_SET_SENSOR_WAKEUP_REQ	请求唤醒传感器节点
0x6001	CMD_NET_CON_RSP	ZigBee 网络连接状态应答
0x6002	CMD_NET_DESP_RSP	ZigBee 网络基本信息应答
0x6003	CMD_NET_TOPO_RSP	ZigBee 网络拓扑信息应答
0x6004	CMD_GET_SENSOR_STATUS_RSP	获得传感器状态信息应答
0x6005	CMD_SET_SENSOR_STATUS_RSP	设置传感器状态应答
0x6006	CMD_SET_SENSOR_SLEEP_RSP	设置传感器休眠应答
0x6007	CMD_SET_SENSOR_WAKEUP_RSP	唤醒传感器节点应答

表 2 协议帧功能码

根据设计中的自定义帧格式，报文中的有效数据被封装成固定格式，通过串口进行传送。开发板和 Coordinator 通过监听串口数据分别对收到得数据包进行解析。解析流程（以 Coordinator 为例）如图 2 所示，具体解析过程如下。

Step1：Coordinator 监听串口（以中断的方式），直到串口有数据。

Step2：读取一个字节，判定是否为自定义帧头。若不是，丢弃数据，回到 Step1。

Step3：读取两个字节，匹配功能码。匹配失败，置错误标志位，丢弃数据，回到 Step1。

Step4：读取一个字节，若该字节数据为 0，则直接跳到 Step6。

Step5：若读到的数据值为 N（0
Step6：读取两个自己数据，对 Step1~5 读到得数据 FCS 校验，若无差错，发送 N 个字节的有效数据给 Z-Stack 协议栈，由 ZStack 协议栈发送给子节点。回到 Step1。

Step7：若 FCS 校验错误，置错误标志位，丢弃已读数据，回到 Step1。

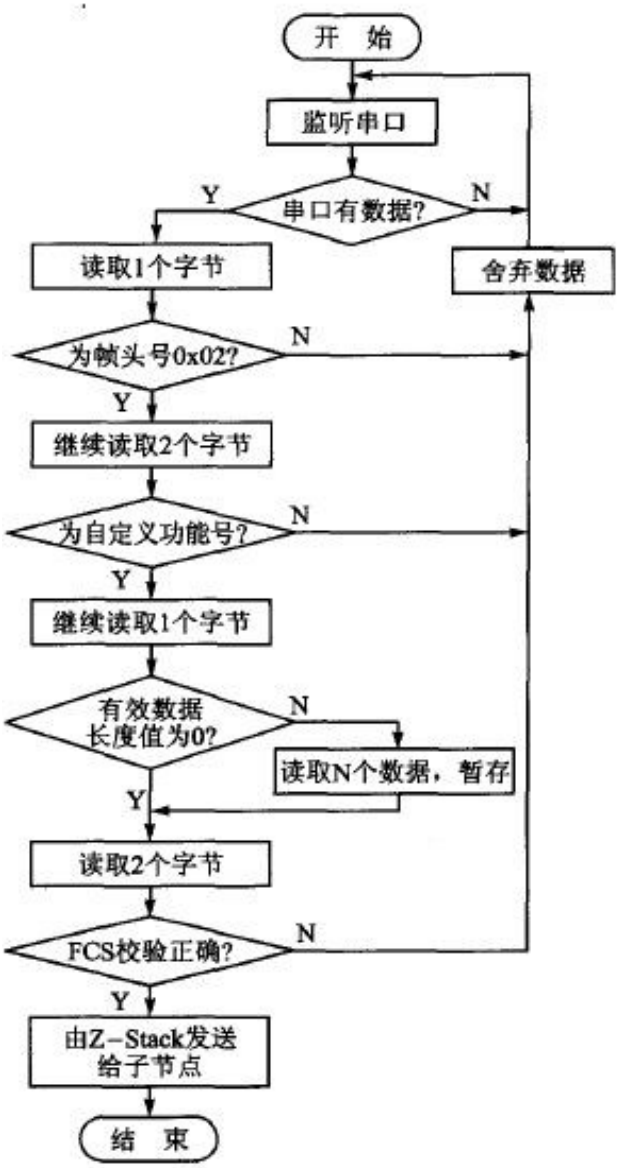

图 2 串口协议解析流程图

3 系统软件设计

3.1 系统软件架构

无线网关软件采用模块化设计，如图 3 所示，由硬件驱动层、操作系统、网络协议层和应用程序组成。硬件驱动层主要描述网关节点中 ZigBee 模块、WiFi 模块以及其他外设的一些驱动；操作系统层移植 ARM Linux，添加无线网卡驱动模块；网络协议层主要包括 ZigBee 协议栈和 WiFi 协议栈；应用程序层主要移植了嵌入式 Web 服务器（BOA）、嵌入式数据库（Sqlite）、CGIC 库和图形化用户界面（Qt）。

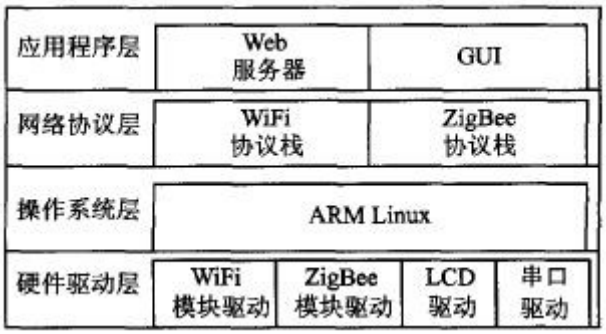

图 3 系统软件架构图

3.2 系统软件流程

根据系统软件架构图，系统软件数据流详细设计如图 4 所示。

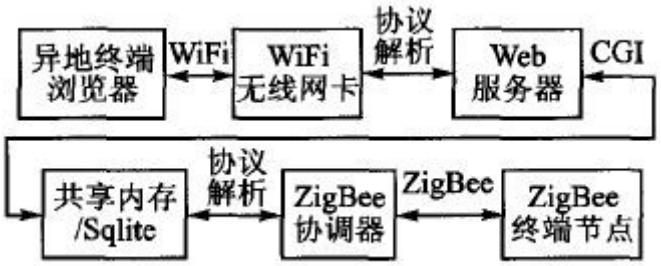

图 4 系统数据流图

以 ZigBee 终端节点发送至异地终端浏览器的数据为例，介绍数据传送的整个过程。当 ZigBee 协调器接收到来自 ZigBee 终端节点的数据后，封装成自定义帧的格式经由串口传送给 Linux 传输协议，经协议解析，将有效数据写入共享内存。当收到外部 Web 请求时，Web 服务器通过 CGI 实时获取共享内存中的数据，并动态更新网页，经由 WiFi 无线网卡以无线的形式传送至终端浏览器。

3.3 测试与验证

利用嵌入式技术对两种协议进行解析，完成协议转换，最终利用手机通过 WiFi 远程访问 Web 页面，读取 ZigBee 终端传感器数据，并对 ZigBee 终端的小灯开关进行远程控制，实现双模网关的基本功能。实验结果如图 5 所示。

图 5 实验结果图

结语

本文通过分析 ZigBee 与 WiFi 协议栈的特点，提出了一种双模无线网关转换的方案，该方案可以很好地完成 ZigBee 组网、远程数据采集和远程控制等任务。实验结果表明，基于 ZigBee 和 WiFi 的双模网关切实可行，可以实现全无线网络的组建，为网络通信从有线向无线过渡提供了一种解决方案。