

Doi:10.3969/j.issn.1003-5060.2013.09.009

一种 ZigBee-TCP/IP 无缝网关模型

王建平, 周辰飞, 朱程辉, 徐晓冰

(合肥工业大学 电气与自动化工程学院, 安徽 合肥 230009)

摘 要: 异构数据通信的研究成为电力集抄系统应用中的关键性技术之一, 文章在分析了 ZigBee 协议栈和 TCP/IP 协议栈的基础上, 给出了 ZigBee 协议与 TCP/IP 协议的地址转换机制和数据格式转换模型, 并由此建立了一个 ZigBee-TCP/IP 无缝连接的网关模型; 通过改进 LWIP 协议栈实现了 ZigBee 协议与 TCP/IP 协议的转化; 最后通过搭建软硬件平台来实现整个网关的设计。

关键词: TCP/IP 协议; ZigBee 协议; 无缝连接; LWIP 协议栈

中图分类号: TP393.3; TP393.4 **文献标志码:** A **文章编号:** 1003-5060(2013)09-1058-05

A gateway model for ZigBee-TCP/IP seamless conversion

WANG Jian-ping, ZHOU Chen-fei, ZHU Cheng-hui, XU Xiao-bing

(School of Electric Engineering and Automation, Hefei University of Technology, Hefei 230009, China)

Abstract: The research on the data communication in heterogeneous network is one of the key technology in the application of electricity reading system. In this paper, based on the analysis of ZigBee protocol stack and TCP/IP protocol stack, an address conversion mechanism and data format conversion model between ZigBee protocol and TCP/IP protocol is provided. Then a gateway model for ZigBee-TCP/IP seamless connection is established. The conversion between ZigBee protocol and TCP/IP protocol is achieved through improving LWIP protocol stack. Finally, the design of the entire gateway is realized through setting up the hardware and software platform.

Key words: TCP/IP protocol; ZigBee protocol; seamless connection; LWIP protocol stack

依据我国电力系统最后 1 km 用电网的技术需求分析, 异构通讯协议转换的研究成为电力集抄系统研究中的一个趋势。

ZigBee 系统设备具有成本低、高可靠、低功耗、环境适应能力强等诸多优势, 在智能电网中具有广泛的应用前景^[1-2]。

近年来国内外学者提出了多种异构网络, 文献[3]在利用现有 GPRS 模块作为数据传输应用的条件下, 对 ZigBee 进行分析研究, 设计出 ZigBee-GPRS 网关; 文献[4]研究了蓝牙与 ZigBee 异构无线网络传输系统中的核心关键技术, 并且给出一个蓝牙与 ZigBee 异构无线网络传输

系统的设计和实现方案; 文献[5]设计了一种 ZigBee MAC 层协议的通讯协议帧模型, 给出了接入到 EPA 架构下控制网络的实现方案, 通过对 ZigBee 接入节点装置的软硬件设计, 实现了基于 EPA 标准的 ZigBee 网络的接入。

本文分析了 ZigBee 协议栈和 TCP/IP 协议栈以及网络通讯的原理, 提出了在 TCP/IP 协议栈的 IP 层与 ZigBee 协议栈的 MAC 层之间创建一个 IP 地址和 MAC 地址的映射表, 在此基础上设计了一个 ZigBee-TCP/IP 无缝连接的网关模型, 并通过改进 LWIP 协议栈实现了 ZigBee 与 TCP/IP 的协议转化。

收稿日期: 2013-01-04; 修回日期: 2013-02-25

基金项目: 国家自然科学基金资助项目(51177034); 安徽省自然科学基金资助项目(2011AKZR1598)和安徽省国际科技合作计划资助项目(11030603014)

作者简介: 王建平(1955—), 男, 河北藁城人, 博士, 合肥工业大学教授, 博士生导师。

1 ZigBee 与 TCP/IP 协议分析

ZigBee 协议是一组基于 IEEE 批准通过的 802.15.4 协议,是有关无线传感器网络组网、安全和应用软件方面的技术标准^[6-7]。ZigBee 协议栈的结构如图 1 所示。

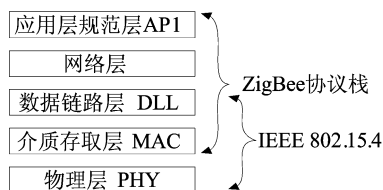


图1 ZigBee 协议栈结构图

1.1 ZigBee 协议的帧结构

ZigBee 物理层数据包由前导码、帧定界符、物理层包头和物理层数据单元组成。其中前导码和帧定界符组成同步包头,用于获取符号同步、扩频同步和帧同步。物理层包头的内容为物理层数据单元的长度。物理层数据单元包含 MAC 层数据包,最长为 127 字节。

MAC 层数据包由帧控制域、帧序号域、地址域、LLC 子层数据包、帧校验组成。帧控制域包含 MAC 帧的类型、地址域的格式以及是否需要接收方确认等控制信息;帧序号域包含发送方对帧的顺序编号,用于匹配确认帧。地址域包含设备的地址信息。

1.2 TCP/IP 协议族

TCP/IP 是 Internet 上的各种系统互连起来的协议族,用于保证数据的准确快速传输。TCP/IP 通常采用一种简单的 4 层模型:应用层、传输层、网络层和数据链路层^[8-9],如图 2 所示。每一层负责的功能如下。

(1) 链路层。通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡,它们一起处理与电缆(或其他任何传输媒介)的物理接口细节。

(2) 网络层。处理分组在网络中的活动,让信息可以发送到相邻的 TCP/IP 网络上的任一主机。在 TCP/IP 协议族中,网络层协议包括 IP、ARP、ICMP 以及 IGMP 协议。ARP 地址解析协议用于将计算机的网络地址(IP 地址 32 位)转化为物理地址(MAC 地址 48 位)。

(3) 传输层。主要为 2 台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中有 2 个

互不相同的传输协议:TCP(传输控制协议)和 UDP(用户数据报协议)。

(4) 应用层。负责处理特定的应用程序细节。

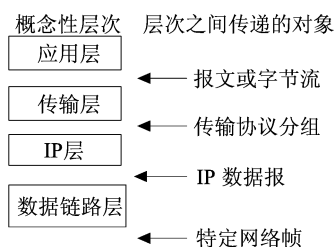


图2 TCP/IP 的分层结构图

在整个协议层次结构中,通信协议使用了复用和分解的技术。发送方在报文中加入报文的类型、选用的协议等附加信息,在接收方收到报文后,参考附加信息对收到的报文进行分解,根据其中的协议类型选择相应的协议进行处理。

2 ZigBee-TCP/IP 协议转换网关逻辑模型

2.1 ZigBee 协议与 TCP/IP 协议的 IP 地址转换

TCP/IP 网络与 ZigBee 网络通信,两者都必须具有唯一的 IP 地址和 MAC 地址。但由于 ZigBee 网络节点没有 IP 地址,只有 64 位 IEEE MAC 地址或者 16 位 ZigBee 网络地址,而根据 TCP/IP 协议的 ARP 可以完成 IP 地址和数据链路层 MAC 硬件地址之间转换的标准,所以可以参考 TCP/IP 的 ARP 实现机制,建立一个 ZigBee 的 MAC 地址到 IP 地址的映射表,分配给 ZigBee 节点一个虚拟的 IP 地址。这样,可以实现 ZigBee 协议中的 IP 地址与 ZigBee 节点 MAC 地址的映射关系。

ZigBee 设备的 64 位 MAC 地址是全球唯一的地址,通常由制造商或者被安装时设置,由 IEEE 来维护和分配。

地址映射表如图 3 所示。

IP地址	64位MAC地址	16位ZigBee网络地址(SADDR)	节点标识符ID
128.128.2.202	0x000000220001	0x1699	0x01
	0x000000220002	0x169A	0x02
	...	...	...

图3 地址映射示意图

2.2 ZigBee 协议与 TCP/IP 协议数据格式转换

ZigBee 协议与 TCP/IP 协议的转换原理如图 4 所示。

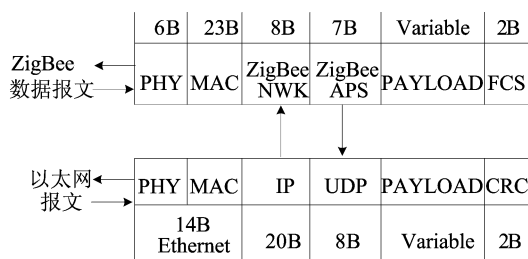


图 4 协议转换图

ZigBee 无线网关协议转换主要是实现 ZigBee 数据报文与以太网报文双向转换。图 4 所示为 2 种协议报文格式转换图。以太网端从网络接口接收一个发往 ZigBee 网关的 IP 数据包;网关路由表控制层经过 ARP 解析后,确定要转发给 ZigBee 网络中的该节点 MAC 地址或网络地址,然后按照图 4 生成 ZigBee 数据包,经由 IEEE802.15.4 物理层将 ZigBee 数据包交至该 ZigBee 节点,如此就完成了从以太网端向 ZigBee 端的协议转换。由 ZigBee 端向以太网端的协议转换与前述过程相反。

鉴于以上原理,现建立一个 ZigBee-TCP/IP 无缝连接的网关模型,如图 5 所示。

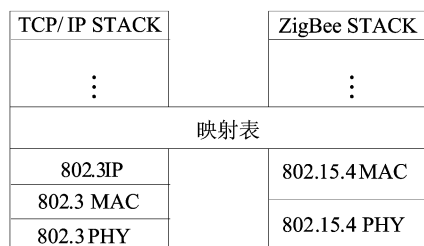


图 5 网关模型图

在 TCP/IP 协议栈的 IP 层与 ZigBee 协议栈的 MAC 层建立一个映射表,当 TCP/IP 需要与 ZigBee 建立连接时,TCP/IP 的 ARP 协议会向 ZigBee 网络发出 ARP 请求,ARP 请求中包括了需要建立连接的 ZigBee 节点的 IP 地址和 MAC 地址,ZigBee 网络通过 ARP 协议从映射表中查找有没有该 IP 地址,如果有就回应一个 ARP 应答,则建立连接。

3 ZigBee 与 TCP/IP 协议转化实现

3.1 LWIP 协议栈的实现

嵌入式实时操作系统 $\mu C/OS-II$ 是一个操作系统内核,本身没有集成 TCP/IP 协议栈,所以需要移植合适的 TCP/IP 协议栈。LWIP 协议栈是适用于 8 位、16 位、32 位微处理器嵌入式系统的

一个小型的 TCP/IP 协议栈,实现了 ARP、TCP、UDP、IP 这些最基本的协议^[10]。

3.1.1 LWIP 协议栈的网络接口设置

LWIP 使用一个与 BSD 中相似的网络接口结构来表示底层网络驱动,结构体的原型定义如下所示。

```
struct netif {
    struct netif * next;
    char name;
    int num;
    struct ip_addr ip_addr;
    struct ip_addr netmask;
    struct ip_addr gw;
    void (* input)(struct pbuf * p, struct netif * inp);
    int (* output)(struct netif * netif, struct pbuf * p,
        struct ip_addr * ipaddr);
    void * state;
}
```

next 指针用于将网络接口链入到全局链表中。name 域用于表示网络接口的类型,只用于这个接口在运行时由人工操作进行配置。name 由设备驱动设置并且应该反映硬件的种类。num 用来区分相同类别的不同网络接口。3 个 IP 地址 ip_addr、netmask、gw 分别用来表示 IP 地址、子网掩码、网关。state 表示设备驱动所包含的网络接口状态,由设备驱动设置。

当设备驱动接受到一个信息包的时候需要调用 input 指向的函数。而网络接口通过 output 指针与设备驱动连接。这个指针指向处于设备驱动中的发送信息包的函数,这个函数将在一个信息包发送出去后,被 IP 层调用。指针 output 将在设备驱动初始化的时候赋值。

3.1.2 LWIP 协议栈的 IP 处理

LWIP 仅实现了 IP 层大部分的基本功能,能够发送、接收以及转发信息包,但是不能接收和发送 IP 分片包,也不能处理携带 IP 参数选项的信息包。对大多数的应用,这不会引起任何问题。

3.2 ZigBee 与 LWIP 协议栈转化

3.2.1 发送信息包

(1) TCP/IP 发送 ZigBee 信息包。当 TCP/IP 网络接收到一个发往 ZigBee 网络的 IP 数据包,IP 层 ip_output_if 函数(需要时,将调用 ip_route 函数进行路由选择)把数据打包、封装,然后调用 ARP 功能解析出该包对应的 ZigBee 网络的 MAC 地址,按照图 4 的数据转换格式生成 Zig-

Bee 数据包,再调用网络接口驱动的 low_level_output 函数传给相应的 ZigBee 节点。

(2) ZigBee 发送 TCP/IP 信息包。当 ZigBee 网络接收到一个发往 TCP/IP 网络的 ZigBee 数据包,ZigBee 协议栈调用 ARP 功能解析出 ZigBee 数据包中对应 MAC 地址的 IP 地址,再调用 TCP/IP 的 ARP 协议解析出自己对应的网络接口地址,然后按照图的格式生成 IP 数据包,TCP/IP 网络接口驱动再通过下述接收信息包的方式接收信息包。

ARP 协议的核心是 ARP 缓存表,ARP 的实质就是对缓存表的建立、更新、查询等操作。ARP 缓存表是由一个个的缓存表项(entry)组成的,LWIP 中的描述缓存表项的数据结构叫 etharp_entry,源代码如下:

```
Struct etharp_entry{
    #if ARP_QUEUEING
        Struct etharp_entry *q;//数据包缓存队列
    #endif
    Struct ip_addr ipaddr;//目标 IP 地址
    Struct eth_addr ethaddr;//MAC 地址
    enum etharp_state state;//描述该 entry 的状态
    u8_t ctime;//描述该 entry 的时间信息
    struct netif *netif;//相应网络接口信息
};
```

3.2.2 接收信息包

(1) TCP/IP 接收 ZigBee 信息包。TCP/IP 网络接口驱动通过 low_level_input 函数读取 ZigBee 端发来的信息包,通常会简单地区分是 ARP 包还是 IP 包,如果是 ARP 包会调用 ARP 功能处理这个包,在 ZigBee 网络发送给 TCP/IP 网络时,发送的一般是 IP 包。所以 low_level_input 函数读到这个数据包的时候会把数据包发送给 ip_input 函数处理,ip_input 函数将数据包进行简单的处理(如计算校验和)后,分析该包是发送到本机的正常数据包,ip_input 则根据包的类型,分别发送给 udp_input、tcp_input、icmp_input 函数处理。如果是发送给 UDP 或 TCP 协议的数据包,UDP、TCP 协议的处理函数将做相应的处理,最后发送给应用程序。

(2) ZigBee 接收 TCP/IP 信息包。TCP/IP 网络发来的信息包是已经转好的 ZigBee 数据包,所以正常接收即可。然后根据 ZigBee 通信协议从 PHY 到 APS 解出其中有效载荷。

如果 ZigBee 网络或 TCP/IP 网络发送的信息包中的目标地址没有相同的网络接口地址,信息包应该被转发。这项工作由 ip_forward() 函数完成。在这里,TTL 字段值被减少,当减为 0 的时候,将会给 IP 信息包的最初发送者发送 ICMP 错误信息,并抛弃该信息包。最后,信息包被转发到适当的网络接口。查找适当的网络接口的算法与发送信息包使用的算法相同。

4 ZigBee-TCP/IP 网关设计

4.1 硬件平台设计

ZigBee-TCP/IP 网关是一个小服务器系统,该系统由 ZigBee 模块、嵌入式服务器和 TCP/IP 接口组成。ZigBee 节点接收到数据后,通过协调器发送给服务器,服务器进行地址和协议转换后发送给 TCP/IP 接口。系统的硬件框图如图 6 所示。

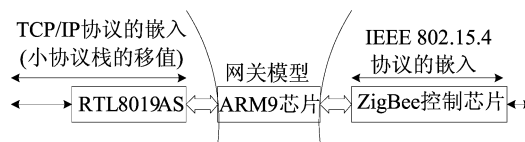


图6 硬件框图

(1) 嵌入式服务器。微控制器采用 ATMEL 公司生产的工业级嵌入式芯片 AT91RM9200,该芯片具有体积小、运算速度快、接口资源丰富的特点。该 CPU 内置 16 K 的 SRAM,128 K 的 ROM;提供 SPI 接口,最多可与 15 个外设通信;提供 10/100 Base-T 型以太网卡接口。通过对微控制器的编程,控制以太网口与 EPA 有线网络进行数据通信。该微控制器还通过 SPI 口与 ZigBee 通讯模块进行通信,控制数据传输。

(2) ZigBee 通讯模块。该模块采用飞思卡尔公司生产的 2.4 G 低功耗射频芯片 CC2420。CC2420 的选择性和敏感性指数超过了 IEEE802.15.4 标准的要求,可确保短距离通信的有效性和可靠性。利用此芯片开发的无线通信设备支持数据传输率高达 250 kb/s,可以实现多点对多点的快速组网。使用该芯片不需要外加单片机来控制,直接用上述的 AT91RM9200 芯片就可以控制。

以太网接口芯片采用 RTL89051AS 芯片,RTL8019AS 是 Realtek 公司生产的以太网接口控制器,符合 Ne2000 标准,遵循 IEEE802.3 协议,支持 8 位、16 位的数据总线,有即插即用、有

跳线、免跳线 3 种工作方式。RTL8019AS 内置 16 KB 的 RAM 用作收发缓冲区以降低对主处理器的请求频率,内部有远程 DMA 通道和本地 DMA 通道。

4.2 软件设计

软件流程图如图 7 所示(以 ZigBee 端向 TCP/IP 端发送为例),主要包括如下 3 个部分。

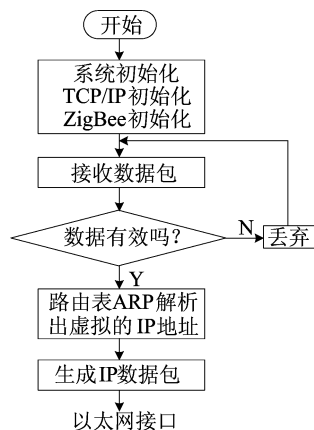


图 7 软件流程图

(1) 初始化。包括各种寄存器的设置,初始化 $\mu\text{C}/\text{OS-II}$, 装载 ZigBee 协议栈以及 TCP/IP 协议栈(初始化 LWIP)。LWIP 初始化需要用到信号量、消息队列等 OS 相关的操作。以下是 LWIP 初始化任务程序。

```

void lwip_init_task(void *pdata)
{
    sys_init(); //用  $\mu\text{C}/\text{OS-II}$  初始化 LWIP 所需的内存块以便使用消息队列通信
    arp_init(); //地址解析协议相关的初始化
    loopif_init(); //环回接口初始化
    mem_init(); //内存初始化
    memp_init();
    netif_init(); //路由表的初始化
    pbuf_init(); //数据报的存储结构的初始化
    stats_init(); //传输状态的初始化
    tcpip_init(); //初始化 tcp, ip, udp 层, 而且建立了主进程
    tcpip_thread
    ne2k_init(); //网络接口的初始化
}
  
```

(2) ZigBee 数据包处理部分。收到数据包判断数据是否有效,无效丢弃,有效拆开数据包,传递到路由表控制层。

(3) 路由表控制层。在 ZigBee 路由表控制层,对 ZigBee 网络内的每一个节点,分配 1 个 IP

网络内的虚拟 IP 地址,将 ZigBee 网络内的节点 MAC 地址映射到 IP 网络内的 IP 地址。TCP/IP 协议的 ARP 协议具有 IP 地址和数据链路层 MAC 硬件地址之间的转换功能,ZigBee 网关可以参照其实现机制来实现 ZigBee 协议栈的 ARP 功能。

5 结束语

本文在深入分析了 ZigBee 协议栈和 TCP/IP 协议栈的基础上,给出了 ZigBee 协议与 TCP/IP 协议的地址转换机制和数据格式转换模型,提出了在 TCP/IP 协议栈的 IP 层与 ZigBee 协议栈的 MAC 层之间创建一个 IP 地址和 MAC 地址的映射表,由此建立了一个 ZigBee-TCP/IP 无缝连接的网关模型;并通过改进 LWIP 协议栈实现了 ZigBee 与 TCP/IP 的协议转化;最后通过搭建软硬件平台来实现整个网关的设计。

该方案的设计使得 ZigBee 网络与 IP 网络融为一体,解决了电能集中抄表系统的扩展兼容性、通讯方式的选择与建设等方面的难题。

[参 考 文 献]

- [1] 肖文,黄虎成,孙茂一,等. ZigBee 技术在智能电网系统中的应用研究[J]. 现代电子技术, 2010, (13): 79-82.
- [2] 何宾,吕育斌,冯涛. Zigbee 技术和 DL/T645 规约在无线抄表系统中的应用[J]. 电力系统保护与控制, 2009, 37(24): 81-84.
- [3] 冼土明. ZigBee 与 GPRS 融合组网技术的研究与应用[D]. 广州: 广州工业大学, 2011.
- [4] 任春雷,李茹. 基于蓝牙与 ZigBee 的异构无线网络传输系统的设计与实现[D]. 呼和浩特: 内蒙古大学, 2011.
- [5] 王建平,徐其林,张茂林. 基于 EPA 标准的 ZigBee 网络构建方法的研究[J]. 计算机测量与控制, 2008, 16(1): 121-123.
- [6] 闫沫. ZigBee 协议栈的分析与设计[D]. 福建厦门: 厦门大学, 2007.
- [7] 王东,张金荣,魏延,等. 利用 ZigBee 技术构建无线传感器网络[J]. 重庆大学学报: 自然科学版, 2006, 29(8): 95-97.
- [8] 史蒂文斯. TCP/IP 详解: 卷 1[M]. 范建华, 曹光辉, 张涛等, 译. 北京: 机械工业出版社, 2000: 1-50.
- [9] 莱特,史蒂文斯. TCP/IP 详解: 卷 2[M]. 陆雪莹, 蒋慧, 译. 北京: 机械工业出版社, 2000: 1-40.
- [10] 张齐,劳焱元. 轻量级协议栈 LWIP 的分析与改进[J]. 计算机工程与设计, 2010, 31(10): 2169-2171.

(责任编辑 马国锋)