Smart Grid 智能电网, 2012, 2, 113-117
http://dx.doi.org/10.12677/sg.2012.24020 Published Online December 2012 (http://www.hanspub.org/journal/sg.html)

Implementation of Wireless Meter Reading System Based on Zigbee and GPRS

Houyun Liu, Yongxiang Liu, Fuhui Hui

Chongqing Electric Power Research and Test Institute, Chongqing
Email: robotcq@gmail.com

Received: Sep. 18th, 2011; revised: Aug. 30th, 2012; accepted: Sep. 10th, 2012

Abstract: A wireless automatic meter reading system is designed based on the Zigbee and GPRS in the paper. The local radio channel is formed by the multi-layer tree Zigbee network, Zigbee network nodes use carrier sense multiple access/collision avoidance (CSMA-CA) algorithm to determine channel usage state. The remote channel is constituted by the GPRS system with security. The wireless automatic meter reading system presented in this paper has strong anti-interference ability, stable and reliable communications for a large number of power systems.

Keywords: Communication Channel; Zigbee; GPRS; Security

基于 Zigbee 和 GPRS 的无线抄表系统研究实现

刘厚云，刘永相，惠富会

重庆电力科学试验研究院，重庆
Email: robotcq@gmail.com

收稿日期：2011 年 9 月 18 日；修回日期：2012 年 8 月 30 日；录用日期：2012 年 9 月 10 日

摘　要：论文基于 Zigbee 和 GPRS 设计了无线自动抄表系统。本地无线信道由 Zigbee 组成的多层树状网络构成，Zigbee 网络节点运用载波侦听多点接入/避免冲撞(CSMA-CA)算法判断信道使用状态，远程信道由 GPRS 构成，系统考虑了安全性并提出了解决方法。系统具有较强的抗干扰能力，通信稳定可靠，适合在中国电力系统中大量推广。

关键词：通信信道；Zigbee；GPRS；安全性

1. 引言

智能电表肩负着电能计量的作用[1]。2009 年，国家电网公司提出建立“坚强智能电网”，智能电表除了计量功能之外，还起着用电客户和电力公司之间双向互动的重要作用[2]。电力公司可以通过通信网络下达停复电通知、调节电费等信息，由此，电力公司可通过智能电表掌握家庭的能耗，甚至通过网络来调控用电客户的负荷，最终实现整个电网的峰谷均衡[3,4]。由此，实现具有双向互动“坚强智能电网”的重要基础就是构建一个稳定可靠的通信信道。

通信信道分为远程信道与本地信道。远程信道有 230 MHz 无线专网、GPRS、CDMA、光纤专网、拨号等多种方式。其中 GPRS 约占 69.56%，230 MHz 无线专网约占 28.43%。在 2005 年以前的相当长一段时间内，由于缺少更适用的通信技术，各地主要选用 230 MHz 无线专网信道实现大用户的数据采集与负荷控制。近年来，随着移动通信技术的发展，GPRS 信道在电力用户用电信息采集得到大量应用。本地信道有电力线窄带载波、RS-485、短距离无线、有线电视网络、电力线宽带载波等多种方式。其中电力线载

波约占 73.7%，RS485 约占 22.7%，其他短距离无线约占 2.0%。电力线窄带载波是目前低压用户采集的主流技术，其通信可靠性及当前载波芯片准不统一是各方关注的问题。各相关方已着手研究提高载波通信可靠性的技术及解决设备互联、互通的方案。RS-485 本地通信技术成熟，通信可靠性高，但由于其运行维护不便，一般采用与电力线窄带载波混合组网的方式。随着技术的发展，电力线宽带载波、433 MHz/Zigbee 等短距离无线等技术也开始试点应用。

目前，有单独采用 GPRS 或 Zigbee 的电能计量设备，但是结合二者的优点，进行综合应用的相关设备还未见报道。

因此论文提出了一种基于本地 Zigbee 信道和远程 GPRS 信道技术构建的自动抄表系统，本地无线信道由 Zigbee 组成的多层树状网络构成，Zigbee 网络节点运用载波侦听多点接入/避免冲撞(CSMA-CA)算法判断信道使用状态，远程信道由 GPRS 构成。系统具有较强的抗干扰能力，通信稳定可靠。

2. 基于 Zigbee 树状网络和 GPRS 技术的无线自动抄表系统

Zigbee 是一种新兴的低功耗、低速率、低成本、低复杂度的无线网络技术。Zigbee 的主要应用领域包括工业控制、消费性电子设备、汽车自动化、家庭和楼宇自动化和医用设备控制等。Zigbee 设备从网络节点逻辑功能上分为终端设备、路由节点和网络协调器，从设备的物理性能上分，可以分为全功能设备和简约功能设备。其中，全功能设备可以充当网络协调器、路由节点或终端设备，而简约功能设备只能充当终端设备节点。因此，从网络逻辑结构上来分析，Zigbee 自动抄表系统内的数据集中器是 Zigbee 网络中的网络协调器，集中器是路由节点，智能电表是终端设备，根据电表的安装位置，也可以设置成路由节点。

智能电表一旦布置，各个节点的相对位置就固定了，考虑此因素，本自动抄表系统的结构采用分层多级树状 Zigbee 网络。协调器为树形拓扑结构顶端节点 A，除了协调器之外每个节点都有其父节点，每个节点都会定时的发送自己的电量数据，数据发送到自己的父节点上，然后再通过父节点继续往上转发，最终到达协调器。协调器要向某个节点发送数据，先将数据传输给子节点，然后再由子节点层层往下传输直到到达指定的节点。各个节点可以判断自己的父节点和子节点和网络状态，具备自组织功能。这种自组织网络的通信方式增加了通信链路的顽固性，提高了整个通信系统的稳健性。

GPRS 无线终端是实现 GPRS 业务的关键设备，起到连接数据采集终端和 GPRS 网络的作用。GPRS 终端将 Zigbee 模块接受到的数据发送至中国移动 GPRS 网络上；接收由 GPRS 网络传输的运行支持系统下发的各项命令，再传送至采集终端。通信网络由 GPRS 无线网络和接入运行支持系统的 Internet 构成，2 个网络之间的互联由中国移动网关实现。运行支持系统对接收的数据进行各项应用处理，并依照这些数据提供各种支持服务和管理功能。这里选择的 GPRS 模块为西门子公司的 MC35I。

基于 Zigbee 和 GPRS 无线通信技术的自动抄表系统结构如图 1 示。该系统由两部分组成，一部分为带 Zigbee 通信模块的智能电表组成的无线传感器网络，另一部分为电力公司数据中心组成的数据网络。这两个网络由 GPRS 联络起来，两个网络能实现双向通信。无线传感器网络中包含带 Zigbee 模块的智能电表和中心节点组成，智能电表除了完成电能的测量外，还具有自组网功能；中心节点一方面可以接受 Zigbee 的数据，另外一方面可以进行 GPRS 无线通信。数据网络除了包含数据库之外，还能接受无线传感器网络中通过 GPRS 发送过来的数据。

3. 系统硬件和软件设计

3.1. 系统硬件设计

智能电表由采集接口、处理器、电源和 Zigbee

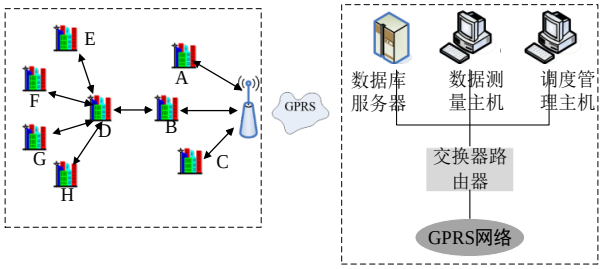

Figure 1. An automatic meter reading system based on Zigbee hierarchical tree network and GPRS network

图 1. 基于 Zigbee 分层树状网络和 GPRS 技术的无线自动抄表系统

射频收发模块组成，原理框图如图 2(a)。采集接口采用可达 0.1%精度的单相电能计量芯片，用来测量用户的电压和电流，并实时计量。处理器采用具有智能控制功能的低功耗单片机，用于测量采集接口的数据并进行计算，同时需要和 Zigbee 模块通信，并管理和协调系统各部分的工作；电源可为处理器和采集接口供电；发射模块用于与外界通信，发送相关信息。中心节点主要起着 Zigbee 和 GPRS 通信功能作用，所以不具备采集接口，原理框图如图 2(b)。

考虑系统的低功耗要求，论文选用 TI 公司的 MSP430F149 低功耗单片机作为处理器，选用 Chipcon 公司的 CC2420EM 射频模块担当无线通信功能。MSP430F149 单片机与 CC2420EM 射频模块接口容易实现且有协议栈支持，处理器芯片具有 60K 在线可编程程序存储器和 4K RAM，完全能植入 Zigbee 协议。

CC2420 是 TI 公司推出的符合 Zigbee 标准的射频收发器，它只需极少外部元器件，性能稳定且功耗极低，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 kbps，可以实现点对点的快速组网。MSP430F149 通过高速 SPI 总线配置和控制 CC2420，其接口电路如图 3 所示。处理器通过 SPI 总线控制和设置芯片的工作模式，并实现读/写缓存数据，读/写状态寄存器等。

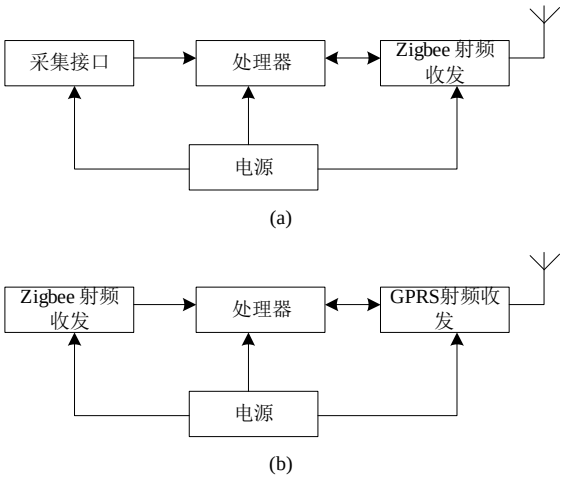

Figure 2. (a) Smart meter; (b) Hardware structure of the central node
图 2. (a) 智能电表；(b) 中心节点硬件框图

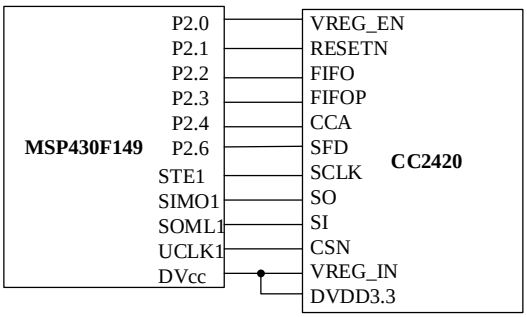

Figure 3. Interface circuit for MSP430F149 and the CC2420
图 3. MSP430F149 与 CC2420 的接口电路

3.2. Zigbee 通信模块的软件设计

完整的 Zigbee 协议由上到下由高层应用规范、应用会话层、网络层、媒介接入控制层和物理层组成。Zigbee 通信模块的软件分 3 部分组成，硬件定义和硬件驱动、SMAC 协议栈和网络层文件。

3.2.1. CC2420 硬件定义和硬件驱动

MSP430F149 通过 SPI 接口配置 CC2420 的工作状态，CC2420 有 33 个 16 位的配置和状态寄存器，15 个命令脉冲寄存器和两个 8 位寄存器分别用于访问发射和接收缓冲器，为了实现可靠的数据传输及网络互联就需要在相应的寄存器中写入适当的值。

3.2.2. SMAC 层协议栈

SMAC 层协议栈主要实现无线信道的数据发送和读取，还可以设置 CC2420 进入和退出休眠状态等。在发送数据之前，Zigbee 网络节点运用载波侦听多点接入/避免冲撞(CSMA-CA)算法判断信道使用状态，一方面载波侦听查看信道是否空闲；另一方面，通过随机的时间等待，使信号冲突发生的概率减到最小，当信道被侦听到处于空闲时，优先发送数据。接收数据由 Zigbee 模块自己完成，一旦开始收取数据，MSP430 处理器进入中断，直到数据收取完成。

3.2.3. 网络层软件设计

设计时参考了自组织网络思想，网络层需要实现以下功能：任何一个节点在上电工作后都能够自动加入网络，即自动找到自己的父节点；任何一个节点的电量等相关信息经过有限跳转后能够到达协调器；任何一个节点以某种原因离开网络的时候，整个网络能够自动愈合。

作为自动抄表系统，节点与节点之间是不需要互相通信的，因此，网络中的每个节点只需要了解自己

周围节点与自己的通讯质量状况，以便通过其中一个节点转发自己的电量信息，节点只需要了解和维护自己周围节点信息的邻居表。在本论文中，邻居表中关于相邻节点的信息只有通过接收相邻节点的数据并分析而得来，这就要求数据帧中含有足够的信息能够帮助其它节点了解该发送该帧的节点信息，同时帧中尽量少有无用子域可以加快节点分析数据的速度。帧结构的设计如表 1 所示。

Typ 用来指明本帧是数据帧、命令帧还是广播帧，数据帧是由电表用户终端发出电表数据；命令帧是由网络中的协调器发出给电表用户终端的命令；广播帧也是由协调器发出以通知周围的节点协调器的存在的数据。Sre 是该帧发送方的 ID 号，本网络中 ID 实际上就是网络 Zigbee 模块的 MAC 地址。Orig 是该帧产生的最初节点的 ID 号。Dest 是该帧应该到达的目的节点 ID 号。Seq 是用来检测无线传输质量的，如节点 A 收到节点 B 传来的帧的序列号是 0x11，下一个收到节点 B 的帧的序列号是 0x13，那么可以判断节点 A 与节点 B 之间通讯丢失了一个帧。Hop 是数据包已经转发经过的节点数，本设计中将最大转发次数设置为 5。Dat 可以是电能数据，也可也是电力公司下发的通知信息或其他命令。

3.3. GPRS 通信软件设计

MSP430F149 是利用 AT 指令来对 MC35I 模块进行初始化、PDP 激活、数据传输的。用户签约 GPRS 业务是以 PDP 上下文为单位的，PDP 是为用户提供 GPRS 数据服务的基本单位，定义了数据传输过程中的用户端地址、服务接入点和 QoS 等重要参数，其中 PDP 类型定义了 PDP 上下文激活期间用户使用的协议类型，目前常用的是 IPv4。

常用的 AT 指令有：

1) 连接到 GPRS 网络：AT + CGATT = 1<CR>。

2) 发起 PDP 上下文激活请求：AT + CGDCONT = 1, IP, CMNET<CR>。

3) 协商 QoS(服务质量)：AT + CGQREQ = 1, 3, 4, 3, 0, 0<CR>。

Table 1. Network layer frame structure
表 1. 网络层帧结构

Typ	Sre	Orig	Dest	Hop	Dat

4) 进行 PDP 上下文激活：AT + CCACT = 1, 1<CR>。

5) 进入数据传输模式：AT + CCDATA = PPP, 1<CR>。

在数据传输的逻辑接口方面，链路层之上是 IP 层，IP 层之上可选的协议主要有面向连接的 TCP 协议和非面向连接的 UDP 协议。当业务的数据要求高可靠性时，应该选用 TCP 协议，但 TCP 协议实现起来复杂，系统负荷太大，UDP 协议没有可靠性的保证，但它的网络负荷小，比较适合实时数据的传输。

4. 基于 Zigbee 网络和 GPRS 无线抄表系统的安全性考虑

基于 Zigbee 网络和 GPRS 无线抄表系统的安全性通过如下两个方面来得到保证。

4.1. Zigbee 通信安全性保障

Zigbee 协议采取了三级安全以防止非法获取数据。最高等级的密码强度采用了高级加密标准(ASE-128)的对称密码，用户可以根据实际情况来灵活调整以确定其安全级别。

4.2. GPRS 通信安全性保障

由于 GPRS 的数据传输处于公共网络环境中，面临着采集数据被窃听，被篡改，传输错误等问题，因此，保证数据的机密性以及数据的可用性是 GPRS 无线自动抄表系统需要解决的问题。

基于 GPRS 的无线自动抄表系统可采用 VPN 系统来保证数据的远程传输的安全。终端通过本地号码或免费号码拨入 ISP，然后 ISP 的 NAS(Net Access Server)再发起一条隧道连接到电力网。

图 4 给出了通过 APN 专线和 VPN 技术相结合接入电力系统内网的网络连接图。主站通过专线和移动公司 GPRS 网的 GGSN 相连，在移动 GGSN 网元上为电力公司设置一个专用的接入 APN 点，从而在终端和电力企业内部网络之间构成一条无线虚拟专网(VPN)通道，解决了电力企业提出的内部网络安全性及数据私密性的要求。移动终端在进行 GPRS 附着时，SGSN 首先向 HLR(Home Location Register 归属位置寄存器)查询移动终端所允许使用的 APN，然后通过

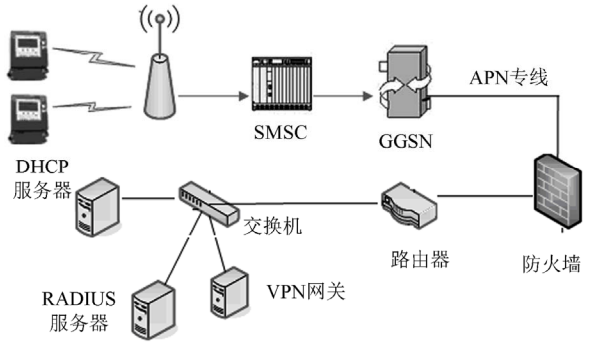

Figure 4. GPRS communications security architecture
图 4. GPRS 通信安全性体系结构

DNS 将 APN 解析成相应的 IP 地址。专用的 APN 在 GGSN 上将体现为专用的网络地址段。由于电力公司通过专线和移动公司连接，此时终端已通过 GPRS 连接到电力系统网上了。

对于专用的 APN，电力公司内部可建立一台 Radius 认证服务器，由电力公司为终端分配帐号和密码。当终端接人企业内部网时，需要通过 Radius 认证，确认用户身份后，才分配 IP 地址。这样，在终端(包括移动设备和 SIM 卡)被盗用时，仍然能够通过用户的帐号和密码保证企业内部网的安全。

5. 结论

论文研究了 Zigbee 和 GPRS 的无线自动电抄表系统。研究了 Zigbee 相关技术在自动抄表系统中的应用。针对电表设计了合理的硬件电路；在软件的实现和设计上，SMAC 协议栈的移植、组网技术和整个网络采用的路由算法并实现是重点；另外实现了 GPRS 通信。在系统的安全性方面，提出了合理的解决方法。本设计能够达到自动电抄表系统的基本要求，电量采集和自组织特性。

参考文献 (References)

[1] 杨少平. 智能电表特点及其应用[J]. 福建建设科技, 2008, 3(81): 91-93.
[2] 帅军庆. 瞄准世界前沿建设智能电网[J]. 国家电网, 2008, 2: 54-57.
[3] 冯迎春. 低谷负荷过载地区的有序用电[J]. 电力需求侧管理, 2008, 10(4): 61-62.
[4] 向阳, 柯有智, 刘五四. 无线专网和公网分层联合通信技术研究[J]. 湖北电力, 2008, 35(4): 53-54.

