



智能家居 433 MHz 射频通信协议栈设计与网关实现

葛 阳¹, 李大刚²

(1. 电子科技大学机械电子工程学院 成都 611731;

2. 电子科技大学中山学院计算机学院 中山 528400)

摘 要: 针对智能家居内部网络低成本、短距离、低数据速率的通信与组网需求, 设计了一种基于 CC1101 的 433 MHz 射频通信协议栈, 并实现了以嵌入式操作系统 $\mu\text{C}/\text{OS-II}$ 与微控制器 STM32F407 为基础的智能网关。该智能网关搭载 Wi-Fi、GSM、网卡等功能模块, 与 433 MHz 射频通信协议栈协调工作实现了多种智能控制方式。详细介绍了 433 MHz 射频协议栈设计、通信协议与节点模型的定义、433 MHz 射频网络组建、数据冲突回避与重发机制。该方案具有简单实用的特点, 适合家庭内部网络使用。

关键词: 433 MHz 射频通信; 智能网关; 433 MHz 射频通信协议栈; CC1101; STM32F407

doi: 10.11959/j.issn.1000-0801.2015216

Design of 433 MHz Communication Protocol and Implementation of Gateway in Intelligence Home

Ge Yang¹, Li Dagang²

(1. School of Mechatronics Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;

2. School of Computer, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528400, China)

Abstract: According to the network establishing demands of the internal network of intelligent home, such as low cost, low data rate, short distance communication, a type of 433 MHz RF communication protocol stack based on CC1101 was created and a gateway based upon the embedded operating system called $\mu\text{C}/\text{OS-II}$ and micro controller called STM32F407 was implemented. This intelligent gateway equipped with Wi-Fi, GSM, ethernet and other functional modules works with the 433 MHz RF communication protocol stack to achieve multiple intelligent controls. Specifically the following points were mainly presented: the design of 433 MHz RF protocol stack, the definition of communication protocol and node model, the establishment of 433 MHz RF network, and the mechanism of date collision avoidance and retransmission. Owing to simplicity and practicality, this scheme is suitable for the application in family internal network.

Key words: 433 MHz RF communication, intelligent gateway, 433 MHz RF communication protocol, CC1101, STM32F407

收稿日期: 2015-05-04; 修回日期: 2015-09-02

基金项目: 广东省产学研结合项目 (No.20118090400556)

Foundation Item: Project Combined with Production and Research in Guangdong Province (No.20118090400556)

论文引用格式: 葛阳, 李大刚. 智能家居 433 MHz 射频通信协议栈设计与网关实现. 电信科学, 2015216

Ge Y, Li D G. Design of 433 MHz communication protocol and implementation of gateway in intelligence home. Telecommunications Science, 2015216



1 引言

无线通信技术是智能家居研究的热点^[1],当今智能家居主流通信技术有 Wi-Fi、ZigBee、蓝牙、433 MHz 射频通信等。针对家庭内部网络低成本、近距离、低复杂度等需求,无线通信技术各有优缺点^[2]:基于 Wi-Fi 技术的智能家居产品多用于数据量较大、传输速率较快的消费电子产品中,其功耗大,成本高;ZigBee 偏向于工业应用,有功耗低、数据量小、网络容量大的特点,适合智能家居这样的碎片化信息传递;蓝牙成本与功耗介于 Wi-Fi 与 ZigBee 之间,适应于短距离的点对点通信,不适合组建庞大的家庭网络。常用的无线通信技术(如 Wi-Fi、ZigBee、蓝牙)工作在 2.4 GHz 频段,日益拥挤的 2.4 GHz 频段信道之间干扰较大。433 MHz 射频通信技术是一种简单而成熟的无线通信技术,其传输距离远、穿墙性强、功耗低、成本低,适用于数据量不是很大、成本敏感的家庭网络^[3-5],其不足之处在于缺乏统一的通信协议规范。

智能家居体系的核心是智能网关,它不仅用于实现各类不同终端设备的集中控制,还起到协议转换作用。本系统智能网关基于 $\mu\text{C}/\text{OS-II}$ 与 STM32F407,设计了一套以 CC1101 通信与组网为目的的 433 MHz 射频协议栈,智能网关搭载 433 MHz 射频模块、GSM 模块、Wi-Fi 模块、以太网模块等,实现了不同方式的集中控制。如图 1 所示,用户可以用手机或者电脑,通过 Wi-Fi、有线等方式登录智能网关嵌入式 Web 服务器,或通过手机 GSM 网络发送短信给智能网关,智能网关解析命令后进行协议转换,通过 433 MHz 射频网络与家电控制终端进行信息交互,达到对家电智能控制的目的。

2 智能家居系统硬件框架

系统总体硬件架构如图 2 所示,智能网关选用

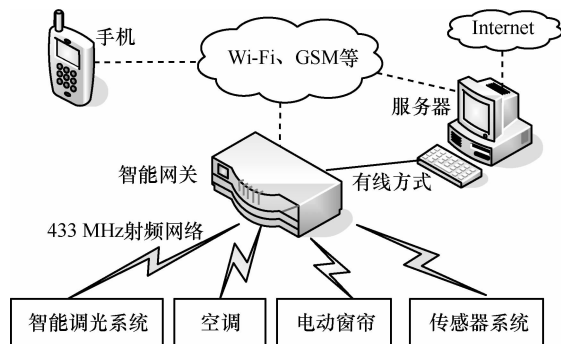


图1 系统框架

STM32F407ZET6,该芯片 SRAM 高达 192 KB,工作主频为 168 MHz,具有丰富的外部资源,可以满足设计需求。Wi-Fi 模块选用的是基于串口 AT 命令的 HLK-RM04,GSM 模块选用 SIM900A,可实现语音、SMS、数据和传真信息的传输。以太网模块选用 PHY 层芯 LAN8720A,通过 RMII 与 STM32F407 的以太网 MAC 层通信。家电端控制节点选择的 MCU 为 STM8S105K4,该 8 位单片机默认主频 2 MHz,满足终端设备数据处理、状态控制等需求。

433 MHz 射频模块选用的是 CC1101,CC1101 是一种低功耗、低成本、传输可靠的无线收发器,工作频段比较灵活,可以设定在 315 MHz、433 MHz、868 MHz 和 915 MHz 的 ISM 和 SRD 频段,空中传输速率可达 500 kBaud。CC1101 是半双工工作方式,只能通过在协议栈软件上进行时分操作,实现 CC1101 时分双工,以更大程度地发挥 CC1101 芯片的性能^[6]。

3 网关软件架构与 433 MHz 射频协议栈设计

3.1 智能网关软件架构

软件是一个系统的灵魂。如图 3 所示,网关的开发采用分层设计的思想,智能网关按其功能,可划分为上层应用软件层、操作系统接口层、底层驱动层。

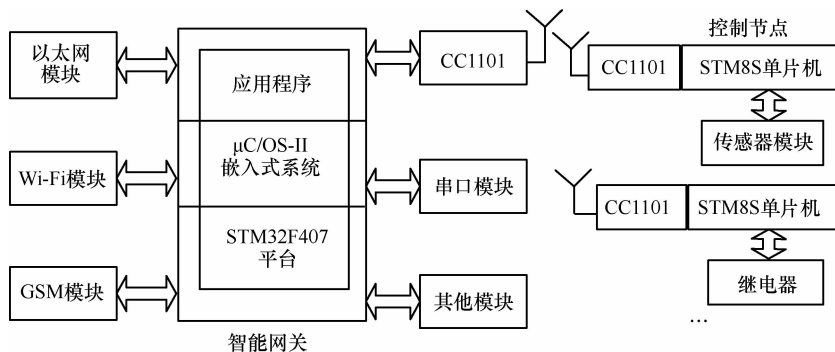


图2 系统硬件框架

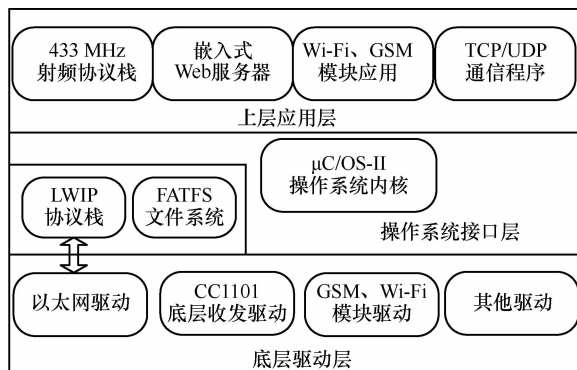


图3 智能网关软件架构

为了提高智能网关的实时性、可扩展性,选用的RTOS为 μ COS-II,同时移植了小型开源的TCP/IP协议栈LWIP^[7],并基于B/S结构在智能网关内部搭建嵌入式Web服务器。FatFs用于在小型嵌入式系统中实现FAT文件系统,它不依赖任何硬件平台^[8],方便智能网关进行数据存储与文件操作。

应用层中433 MHz射频协议栈是核心部分,它用来实现家庭内部433 MHz射频网络的组建与通信。上层应用层中的嵌入式Web服务器、Wi-Fi、GSM等应用进程提供了用户与智能网关不同的交互方式,底层就是与硬件交互的驱动层,如CC1101底层的数据收发函数,以太网卡通信驱动等。底层驱动程序应该做到精简、高效,因为底层驱动的执行效率直接关乎系统的实时性,进而影响整个系统的性能。

3.2 433 MHz 射频协议栈设计

433 MHz 射频协议栈总体架构如图4所示,总体上协

议栈分为用户空间与内核空间。

用户空间是具体的应用进程,如嵌入式Web服务器进程、Wi-Fi应用进程、串口应用进程等,由于空间所限没有标明GSM进程。这4个进程处于用户空间,进程优先级相对内核空间进程较低,各应用进程接收来自如Wi-Fi、网页浏览器、串口等消息,进行解析后封装成内核能识别的rf_message消息结构体,通过API函数与内核通信。重要的数据结构,如应用进程RF_PCB链表、终端控制节点PCB链表等,只有内核空间才能访问与修改,用户空间无法触及,应用进程只能通过API函数进入内核,在内核中安全访问,减少用户空间恶意修改内核核心代码造成的损失^[9]。这样既保证了协议栈与数据通信的安全性,又简化了应用进程的设计难度,应用进程只需要调用内核API函数即可完成相应的功能。

在用户空间中,应用进程的创建会分配进程控制块,含有进程的相关信息,各个进程控制块组成RF_PCB链表module_pcb_list,记录活动的应用进程。进程控制块记录应用进程运行状态、收发的数据队列、数据帧时间戳等,是各个应用进程的高度抽象。

内核空间重要的是RF核心进程rf_core_thread(),它控制网络层中数据帧的路由,链路层中数据分组的发送接收等功能,向上与应用层的进程完成用户空间与内核空间的信息交换,向下与底层的发送、接收、轮询等进程交互,完成物理层的功能。消息队列rf_core_mbox是核心进程rf_core_thread()与其他进程通信的核心,也是API函数实现

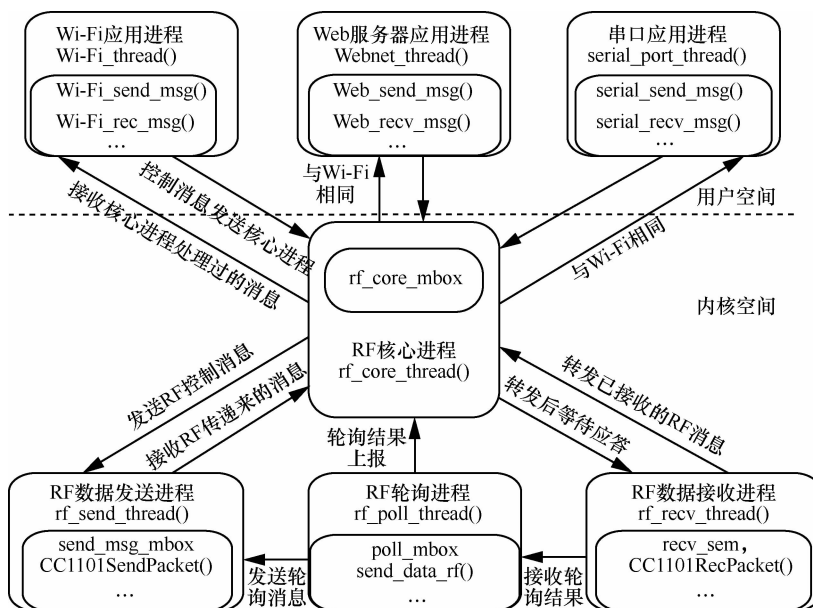


图4 433 MHz 射频协议栈总体架构



的基础,RF 核心进程 `rf_core_thread()` 在消息队列 `rf_core_mbox` 上等待消息到达,该消息结构体中封装了协议帧、控制信息、API 函数等,核心进程利用其中的 API 函数对消息帧进行解析。

核心进程与底层收发、轮询进程的交互过程类似。RF 数据发送进程 `rf_send_thread()` 通过消息队列 `rf_send_mbox` 接收核心进程的消息,处理过后通过 `CC1101SendPacket()` 函数进行物理层数据发送。`CC1101` 的数据接收是通过中断方式, `CC1101RecPacket()` 接收数据分组,接收进程 `rf_rcv_thread()` 经过处理后上传给核心进程 `rf_core_thread()`。RF 轮询进程每隔一定的时间就会给控制节点发送轮询数据帧,控制节点接收到后应答,智能网关通过此方式对节点的存活进行确认。

4 433 MHz 射频网络整体模型

4.1 网络拓扑与组网过程

基于家庭内部通信与组网的特点,本系统选择树型网络,如图 5 所示。节点分为 3 类:智能网关节点、中继节点和控制节点。智能网关节点是整个网络的核心,每个控制节点(如灯光控制节点、空调控制节点等)在上电之后会进行入网操作,向智能网关发送入网请求,智能网关根据请求组建树型网络,协议栈构建与维护控制节点链表。

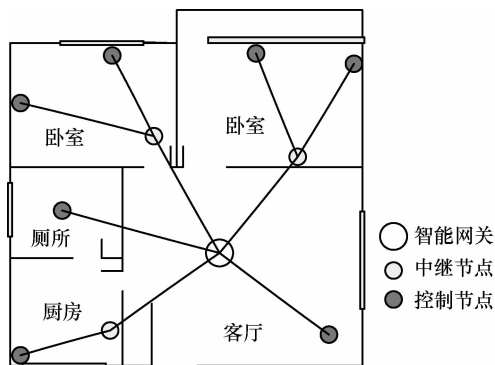


图 5 系统无线网络拓扑

智能网关与节点采用双向通信的方法进行通信。客厅内的节点与智能网关节点距离较近,采用直接通信的方法进行通信。处于其他房间的控制节点,由于传输距离较远,加之中间有墙壁阻挡,需要中继节点参与传输,这就需要一定的路由机制,鉴于低复杂度的目的,这里的路由路线是固定的。智能网关节点与卧室或者厨房内的控制节点通信时,智能网关发送数据分组给目的房间内的中继节点,中继节点接收到数据分组进行解析,转发给目的控制节

点,完成一次单向通信。

433 MHz 射频网络组建如下:当智能网关上电或者重启之后,网络重新组建,智能网关监听入网帧。控制节点或者中继节点上电后发送入网帧,入网帧包括该节点的 ID 与位置信息,节点发送入网帧之后等待智能网关的入网答复帧。智能网关收到入网帧之后,进行入网节点信息分析,确定节点在树型网络中的位置,注册终端控制节点结构体,之后给入网节点发送入网答复帧,控制节点接收到入网答复帧之后,分析确认自己所处的树型网络位置,之后进入正常处理流程,否则会休眠一段时间之后继续发送入网帧。

智能网关感应树型网络的动态变化,实时更新树型网络中的节点信息,智能网关每隔一定的时间会发送轮询数据帧,并等待节点的应答,若在一定时间内,控制节点没有应答,则说明该节点出现问题或者位置信息发生变化,网络信号无法覆盖,智能网关删除在活动链表中无应答的节点信息,更新树型网络结构。

4.2 433 MHz 射频节点模型与通信帧定义

本系统对 `CC1101` 节点之间的通信帧进行了详细的设计,如图 6 所示,节点模型由物理层、链路层、网络层、应用层组成,每一层为上一层提供服务,并使用下一层提供的服务完成相应的功能^[10]。

物理层与链路层由 `CC1101` 芯片提供,完成节点之间基本的数据帧的发送与接收功能,物理层数据帧发送时,自动生成前导码与同步词汇,实现节点数据帧同步。数据帧在链路层中,收发地址手动添加,接收地址可能是最终要到达的目的地址,也可能是中继地址。当设定 `CC1101` 寄存器 `PKTCTRL1.append_status` 值为 1 时(默认为 1),`CC1101` 芯片在数据发送时会默认追加 RSSI 与 LQI 状态值,RSSI 是信号强度指示值,从该值可以获取当前信道的信号强度与干扰,LQI 是当前接收信号的质量指示。`CC1101` 芯片会自动添加 CRC 字段,确保除前导码、同步词汇、RSSI、LQI 之外的数据正确性与完整性。

网络层完成树型网络中任意节点与智能网关的数据通信,配合链路层完成路由功能,网络层中数据帧中源地址是数据产生的源节点,目的地址是数据最终要到达的节点。应用层定义了通信帧的具体功能,参数定义了节点的具体动作(如调节空调温度、灯光亮度等),端口号识别用户空间不同的应用进程,实现了节点之间的服务与资源共享。

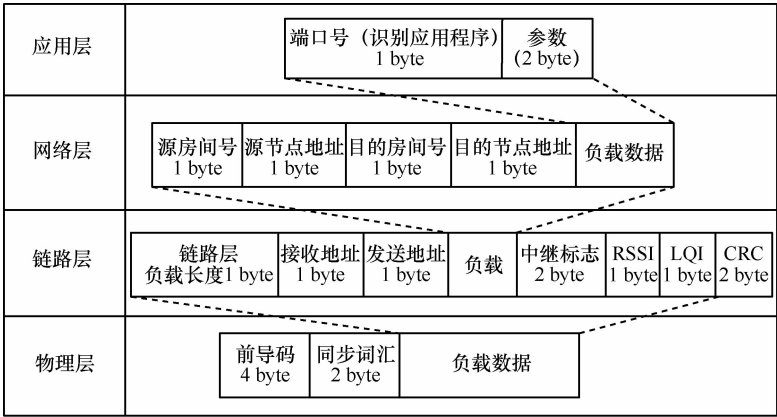


图 6 节点模型与 433 MHz 射频通信帧定义

5 通信过程实现

本系统选择射频通信工作在 433 MHz,该频段不用申请即可以免费使用.CC1101 工作在 433 MHz 频段时,频率波段为 400~464 MHz,信道频间(信道带宽)为 200 kHz,可用信道达 300 个.由于树型网络中所有节点都工作在同一信道,并且 CC1101 芯片是半双工,所以同一信道的通信碰撞是无法避免的,这就需要一定的机制实现冲突退避与数据重发^[1].冲突检测采用 CC1101 硬件实现,退避与重发在冲突检测基础上,通过协议栈软件实现.

5.1 冲突退避的实现

CC1101 数字引脚 GDO2 用于载波监听时,当所在信道中 RSSI 值高于设定的阈值时,GDO2 引脚输出高电平,也就意味着当前信道正在使用.通过 GDO2 引脚电平判断信道状态,通过协议栈进而实现冲突退避.

冲突退避实现方式如下.当检测到数据冲突时,则进行一定的时延机制后再次检测,信道空闲则进行发送.在协议栈中,根据节点的地址设置重发间隔,由于各节点的地址不同,数据重发的时刻也不同,则两个节点同时发送数据导致冲突时,重发时刻也不同,重发数据能够成功.同时,设定重发最小时间间隔大于最大数据分组的传输时间,保证重发数据分组与其他节点无重合时间.根据 433 MHz 射频通信帧的定义,数据分组长度为 22 byte,即 176 bit,空中传输速率为 200 kbit/s 时,空中传输时间为 880 μs,加上 CC1101 状态机的转换,由接收态 RX 转换为发射态 TX (CC1101 中断接收需要使芯片处于 RX 状态),所需时间约为 600 μs,则发送一次数据总的时间开销约 1.5 ms,即重发最小时间间隔为 1.5 ms.如果某一节点的重发时间为 T_{ms} ,该节点地址为 $addr$,则该节点重

发时间间隔为 $T=addr\times1.5$.

5.2 数据重发机制

数据重发是在冲突检测与退避的基础上实现.如图 7 所示,433 MHz 射频网络中的数据通信要求可靠性,这就需要节点消息应答,如果智能网关控制信息发送后,在规定的时间内没有收到节点的应答,则消息要进行重发.

协议栈的数据发送 `rf_send_thread()` 进程中,在实际发送前,首先进行冲突检测,若信道冲突,则进行冲突退避机

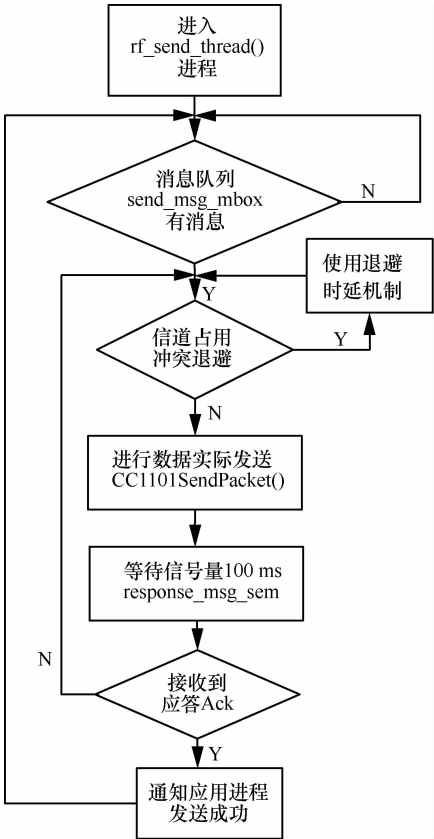


图 7 数据重发流程



制,信道空闲使用 CC1101SendPacket()函数进行物理层的消息发送。发送完成后,该进程通过 response_mg_sem 信号量等待节点应答,协议栈在接收到应答消息后,在中断处理函数中增加信号量,rf_send_thread()进程完成一次数据发送过程,若该进程在 100 ms 内没有接收到应答消息则再次发送,在规定的次数中没有接收到应答,则通告应用进程消息发送失败,节点无应答。

5.3 433 MHz 射频网络工作流程

整个 433 MHz 射频网络要遵循一定的通信逻辑,如图 8 所示(为描述方便,省略中继节点转发),主要分为以下 4 个部分。

- 初始化与网络组建:智能网关与智能节点上电后进行初始化工作,智能网关监听入网帧,控制节点入网注册,入网后控制节点进入正常工作流程。
- 主动控制:手机或者电脑端发送控制命令,智能网关接收后进行解析,通过 433 MHz 射频网络发送至相应的控制节点,控制节点执行后反馈。
- 控制节点状态上报:控制节点状态改变或者有信息需要主动上报时,智能网关接收上报信息,进行分析与处理,并反馈给用户空间进程。
- 智能网关轮询与节点删除:智能网关中轮询进程 rf_poll_thread() 每隔一定的时间就会发送轮询信息至各个控制节点,控制节点应答,智能网关接收到应答后证明该控制节点工作正常,如果没有接收到应答,则说明该节点出现故障或者主动离开,智能网关更新树型网络结构。

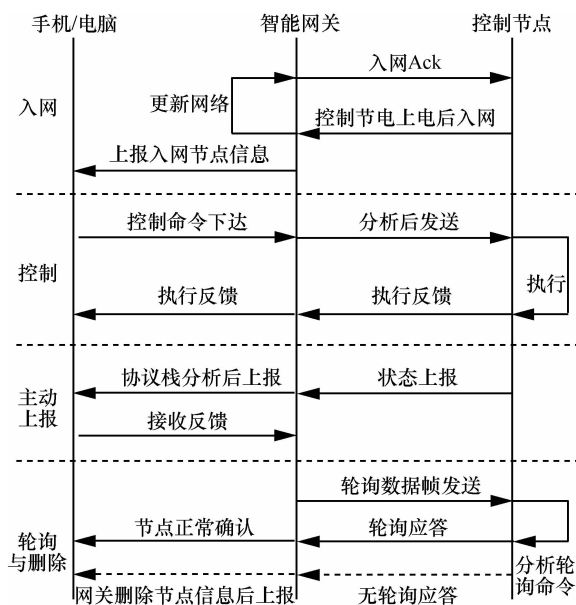


图 8 433 MHz 射频网络通信流程

6 实验结果

测试表明,射频芯片 CC1101 输出功率设置为 0 dB 时,电流消耗为 15.9 mA,传输距离为 15 m,具有良好的穿透能力。图 9 为测试结果,当通过浏览器发送客厅灯光亮度 1 指令给智能网关后,智能网关通过 433 MHz 射频网络将消息发送至智能调光系统,家电控制终端的状态通过 433 MHz 射频网络反馈给智能网关,智能网关通过 SSI 技术在浏览器中显示状态。

用户中心	房间1当前状态	
	当前温度	28℃
	火源检测	OK
	电动窗帘	关
	灯光系统	亮度1
	安全退出	

图 9 实时信息显示

7 结束语

本文设计了一种适合家庭内部网络使用的 433 MHz 射频通信协议栈,并详细讨论了协议栈的工作原理。在下一步工作中,会继续增加家电控制终端,完善协议栈的设计,提高系统的稳定性。

参考文献

- 1 Sujatha D C, Satheesh A, Kumar D, *et al.* Intelligent infrastructure at home using internet of things. *Advances in Intelligent Systems and Computing*, 2014, 49(2): 627~634
- 2 Zheng Y H. An analysis on wireless communications technology in intelligent home. *Proceedings of 2011 International Conference on E-Business and E-Government*, Shanghai, China, 2011: 1~4, 6~8
- 3 贺安坤,张亮,宋长青等. 基于 ZigBee 技术的智能家居系统的设计与实现, *微计算机信息*, 2012(9): 4~6
He A K, Zhang L, Song C Q, *et al.* Design and implementation of smart home system based on ZigBee technology. *Microcomputer Information*, 2012(9): 4~6
- 4 Zheng T, Wang S, Kamel A E. Bluetooth communication reliability of mobile vehicles. *Proceedings of 2011 International Conference on Fluid Power and Mechatronics*, Beijing, China, 2011: 8~17
- 5 涂亮. 基于 433 无线收发模块的物联网智能家居系统设计. *电视技术*, 2012, 36(6): 44~46
Tu L. Design of smart home system based on 433 wireless transceiver module. *Video Engineering*, 2012, 36(6): 44~46

- 6 TI. CC1101 low-power sub-1GHz RF transceiver. <http://www.ti.com.cn/en/lit/ds/symlink/CC1101.pdf>.
- 7 胡俐蕊, 王则林, 胡传志. 基于 LwIP 的 μ C/OS-II 网络应用程序设计方法. 计算机应用与软件, 2010, 27(4): 54~57
Hu L R, Wang Z L, Hu C Z. Method of network application programming in μ C/OS- II based on LwIP. Compute Applications and Software, 2010, 27(4): 54~57
- 8 邓昀, 程小辉, 王新政. 微内核结构嵌入式实时操作系统的研究与设计. 微电子学与计算机, 2012, 29(10): 133~139
Deng Y, Cheng X H, Wang X Z. Study and design of embedded real-time microkernel operating system. Microelectronics and Computer, 2012, 29(10): 133~139
- 9 Israeli A, Feitelson D G. The linux kernel as a case study in software evolution. Journal of Systems and Software, 2010, 83(3): 485~501
- 10 李志宇, 史浩. 无线传感器网络微型节点的实现. 电子产品世界, 2005(11): 115~117
Li Z Y, Shi H. The implementing of wireless sensor network node. Electronic Engineering & Product World, 2005 (11): 115~117
- 11 杨旭, 李德敏, 张谦益. 基于 nRF24L01 的一种无线通信协议

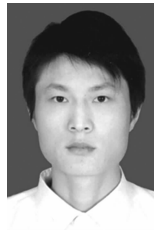
设计. 通信技术, 2011, 44(7): 57~59

Yang X, Li D M, Zhang Q Y. A design of wireless communication protocol based on nRF24L01. Communications Technology, 2011, 44(7): 57~59

[作者简介]



葛阳, 男, 电子科技大学硕士生, 主要研究方向为物联网智能家居。



李大刚, 男, 电子科技大学中山学院助理研究员, 主要研究方向为嵌入式系统研究与开发。