基于 ZigBee 的 LED 路灯固件远程在线升级研究*

任 彧,郭太磊
(杭州电子科技大学 软件与智能控制研究所,浙江 杭州 310018)

摘要:为了有效降低嵌入式系统的升级和维护成本,根据嵌入式设备存储结构和更新原理,提出了一种基于 ZigBee 的固件远程在线升级技术,包括在应用编程(IAP)在线升级、ZigBee 协议的改进、片上 Flash 分区、应答机制、断点续传技术和滑动窗口协议。结合远程在线升级策略在 LED 路灯节能控制系统中的应用试验,详细阐述了远程固件在线升级流程。研究结果证明,该方案具有快捷简便、硬件成本低、通信误码率低的优点,具有广阔的应用前景。

关键词:ZigBee;在线升级;在应用编程;LED 路灯节能系统
中图分类号:TM923.4;TP393.17 **文献标志码**:A **文章编号**:1001-4551(2012)01-0120-04

Remote online firmware updating method used in LED street lamp energy-saving system based on ZigBee

REN Yu, GUO Tai-lei
(Institute of Software and Intelligence, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: In order to reduce the embedded system upgrade and maintenance costs effectively, according to the embedded equipment storage structure and updating principle, a remote online firmware updating technology based on ZigBee was proposed, including in application programming(IAP) online upgrade principle, improvement of ZigBee protocol, flash zoning on chip, response mechanism, breakpoint resuming and sliding window protocol. Combined with remote online firmware updating strategy used in LED street lamps energy-saving system, a technological process of the remote online firmware upgrade was described. The research result proves that this design scheme has a simple and easy to use characteristic. Beside, it helps to reduce the hardware cost and communication error rate, has vast applied foreground.

Key words: ZigBee; online upgrade; in application programming(IAP); LED street lamp energy-saving system

0 引 言

嵌入式产品在投入使用阶段由于各种原因需要对产品进行维护或者软件升级,若使用传统的本地程序更新方式,需要对产品进行召回处理,增加了企业成本。如果嵌入式产品放置在极端恶劣的环境下,传统的升级方式无法进行。因此,研究嵌入式产品的固件在线升级就显得尤为重要。

按升级数据的传输方式不同,目前嵌入式系统常用的在线升级方法可分为有线传输和无线传输。常见的有线传输方式是基于串行电缆[1]和以太网[2]的连接传输。有线传输性能稳定,使用方便,但升级节点和服务器端之间需要架设一条专用电缆或网线(配备网卡),成本较高;常用的无线传输方式有基于 GPRS/CDMA 的数据传输[3]和基于无线传感器网络的数据传输[4-5]。借助 GPRS/CDMA 连接到互联网,网络升级方便可靠,但通信模块昂贵,需要额外支付数据流量费。无线传感器网络的升级大多依赖操作系统提供的 bootloader,该方法代码维护方便、准确率高,但升级操作较复杂,操作系统对硬件要求较高。

本研究提出一种基于 ZigBee 的嵌入式系统的远程固件在线升级技术,并以笔者参与设计的 LED 路灯

收稿日期:2011-06-21
基金项目:浙江省重大科技专项重点工业资助项目(2011C11092)
作者简介:任 彧(1963-),男,浙江上虞人,教授,硕士生导师,主要从事计算机智能控制、计算机网络技术方面的研究. E-mail:renyu@hdu.edu.cn

节能系统中的固件远程在线升级方案为例,介绍了在线升级的过程。

1　概述

该固件远程升级中,升级代码无线传输使用的是 ZigBee 协议。ZigBee 是一种无线网络协定,由 ZigBee Alliance 制定(从 1998 年开始发展),底层是采用 IEEE 802.15.4 标准规范的媒体存取层与实体层。其主要特点是低速、低耗电、低成本、支持大量网络节点、支持多种网络拓扑、低复杂度、快速、可靠、安全。ZigBee 网络中的设备按照功能的不同可以分为协调器(coordinator)、路由器(router)和终端节点(enddevice)。其中,ZigBee 协调器作为网络的发起者和维护者管理整个 ZigBee 网络,通过路由器的连接中继作用,协调器可以控制超出它能量覆盖范围的设备。

在 LED 路灯无线节能系统中,路灯网络为双向长狭状拓扑,路灯以路由器的身份加入到协调器建立的 ZigBee 网络中。协调器节点首先发起升级会话,通过无线收发装置,以多跳的形式向路灯节点注入升级代码。路灯节点收到升级代码后使用在应用编程(IAP)技术将新代码写入指定的 Flash 升级代码区,重启之后运行新代码,完成升级过程。

2　在线升级理论基础

2.1　在应用编程

在应用编程(IAP)是应用于 Flash 程序存储器的一种编程模式,通过使用这种方法可以在应用程序的控制下对程序存储空间进行读取、擦除、写入操作。这意味着处理器在执行用户应用程序时可以更换执行代码,甚至自己生成代码,具有在线升级的功能。相比于传统的在系统编程(In System Programming)方式,在应用编程不需要开发人员进行现场操作,因而具有更广阔的应用前景。

IAP 是通过运行处理器中的用户代码对 Flash 程序存储器进行擦除和写入操作的。当被写入的数据为待更新的程序代码时,就可以实现在线升级。

2.2　基于 ZigBee 的代码传输

ZigBee 是一种低速无线个域网技术,通信数据量不大,数据传输速率相对较低,但可以提供安全、可靠的数据传输,要求成本和功耗非常低,并容易安装使用。ZigBee 在物理层和媒体访问层采用 IEEE 802.15.4 协议,使用带时隙或不带时隙的载波检测多址访问与冲突避免(CSMA-CA)的数据传输方法,并与确认和数据检验等措施结合,可保证数据的可靠传输。安全性是 ZigBee 的另一个特点。为了提高灵活性和支持在资源匮乏的 MCU 上运行,ZigBee 支持 3 种安全模式,最高级的安全模式采用属于高级加密标准(AES)的对称密码和公开密钥[6]。

2.3　系统检测关键点

为了便于对升级进行管理,本研究在方案中引入一个升级管理区。升级管理区负责记录管理升级事务,如版本维护数量、出厂默认版本的跳转地址、跳转目标固件版本的地址、下次升级代码的下载地址和断点续传信息等。引导程序通过读取升级管理区,可确定当前版本号和下一步跳转地址,最后跳转到相应的用户应用程序代码区。

2.4　断点续传技术

断点续传就是在上一次连接断开的位置开始继续下载。在系统升级过程中,可能出现设备故障、通信故障等传输中断或升级会话中断的问题,一般的解决办法是重建连接后,路灯节点请求全部重传升级文件。为避免重复传输升级数据,本研究在固件升级协议中引入断点续传功能。

在 HTTP 协议中,断点续传的实现是在请求报头中加入 Range 段,表示客户端希望从何处继续下载[7]。本研究参考 HTTP 协议,在 ZigBee 升级帧中加入帧序列号,并记录断点帧序列。当升级会话重新启动时,路灯节点直接从断点处请求升级序列帧。

3　LED 路灯在线固件升级设计

本研究所述的硬件平台是自行开发的 LED 路灯网络节点。主要模块使用 STM32F103CB 和 SN260。其中,STM32F103CB 是基于 ARM Cortex-M3 的 32 位嵌入式处理器,拥有 128 KB 的高速可编程 Flash 存储器;SN260 是 ZigBee 模块,负责组网和升级数据传输。

3.1　Flash 分区和 IAP 编程

路灯节点片内 Flash 中有两类区域:引导代码区和升级代码区。引导代码主要起引导作用,位于复位的起始地址;升级代码区可以存储不同的代码版本,按升级代码镜像文件的大小和上述硬件平台的限制,路灯节点共存储 4 个固件版本。

片内 Flash 分区如图 1 所示。

IAP 编程的实现主要依赖 ST 公司的固件函数库 stm32f10x_flash。开发者可以调用该函数库实现 Flash 页面读/写和擦除功能。例如:FLASH _ ErasePage (uint32_t Page Address)函数可以擦除指定位置的页

面;而 FLASH_ProgramWord(uint32_t Address, uint32_t Data)函数可在某指定地址写入一个字(32 位)。

执行 IAP 编程时应该首先对 Flash 解锁,然后判断有无读/写保护,如果有保护的话首先关闭读/写保护。关保护成功后,首先擦除指定的 Flash 页,之后对该页进行 IAP 编程。编程结束后,对已编程的 Flash 页进行校验以验证是否写入成功[8]。

3.2 引导程序执行

引导程序的执行流程如图 2 所示。

引导程序首先读取升级管理区,选择加载的升级程序版本并找到该版本的中断向量表;从中断向量表中读取堆栈初始地址和主函数地址后,升级程序重新初始化堆栈并完成中断向量表重映射,最后跳转到主函数处执行。

为使引导程序正确找到升级程序的中断向量表,需要重链接升级程序,新链接地址与如图 1 所示的 Flash 分区表保持一致。通过使用 ST 固件函数库中函数 NVIC_SetVectorTable ( )可设定升级程序中断向量表的位置。

图 1 Flash 存储分区

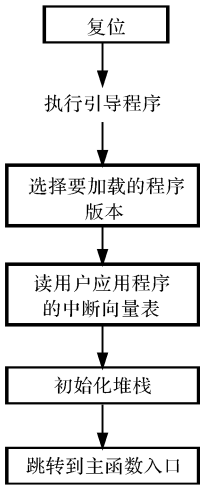

图 2 引导程序流程图

3.3 ZigBee 协议的改进

ZigBee 协议的应用层帧结构由几个部分组成:帧控制域、目的端点、簇标识符、模版标识符、源端点和帧载荷。为满足在线升级的需要,本研究对 ZigBee 协议做了一些改进,在应用支持子层上嵌入了一个自定义的固件升级协议,主要改进如下:

(1)增加了重发和确认返回机制。在更新过程中,每发送一帧数据都需要返回确认。当出现丢帧时,控制器要求重发,3 次出错后系统报错,停止传输。

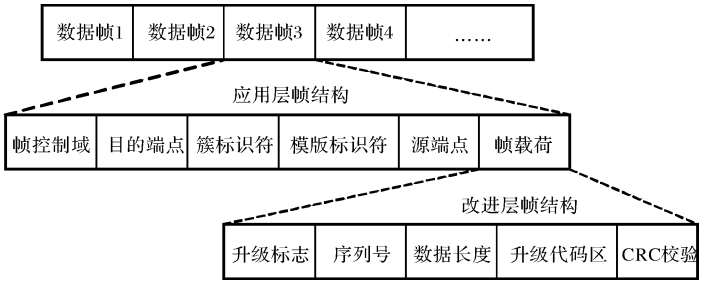

图 3 ZigBee 升级帧结构

(2)为保证数据传输质量的同时兼顾传输效率,引入滑动窗口协议[9]。本研究在发送端和接收端分别设置发送、接收窗口。其中,发送窗口进行流量控制,其大小表示发送端在未收到确认帧的情形下一次最多可以发送多少个单位的数据帧。接收端只接收落入接收窗口内的升级帧。

(3)增加断点续传功能。如前文所述,客户端升级管理页面记录故障标志、断点处的帧序列号、故障原因等信息,当连接重新建立后,客户端从上次升级断点处继续请求接收升级数据包,而不需要重新下发,可提高数据利用率。

(4)为有效支持上述功能,本研究需要在每帧数据的帧载荷区域加入若干控制域,如升级标志、发送序列号、数据长度和 CRC 校验码等。

4 固件升级流程和实验验证

基于 ZigBee 的固件升级流程如图 4 所示。具体升级步骤如下:

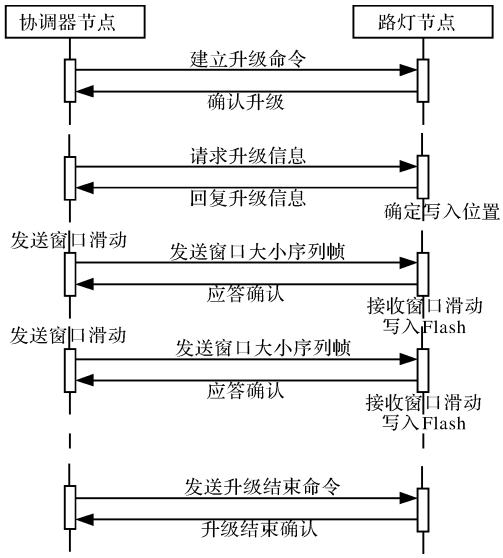

图 4 固件升级流程

(1)协调器节点发起固件升级连接命令,路灯节

点收到后响应该命令。

(2)协调器节点需要知道路灯节点的升级信息,如上次断点处、故障原因等,向路灯节点请求升级信息;路灯节点回复本地升级信息,并确认升级程序的写入首地址。

(3)若协调器节点从路灯升级信息里读出故障信息,则升级程序从断点序列号处开始发送;若没有故障信息,则从升级程序的序列号 1 开始发送。

(4)协调器节点发送一个窗口大小的代码帧,收到与当前窗口序号一致的应答时,发送窗口滑动,继续下一窗口的帧序列发送。

(5)升级镜像文件传送完毕后,协调器节点发送升级结束命令,路灯节点收到该命令后,修改升级管理区,更新版本号、跳转目标固件版本的地址、下次升级代码的下载地址等信息。

(6)若中途帧序列发生故障,路灯节点在 3 个等待周期结束后,修改升级管理区,更新断点续传信息(故障原因、下次接收帧序列号)。

实验使用的硬件平台为前述的 LED 路灯网络节点,所取网络频段为 2.4 GHz 的 17 信道,数据传输速度为 250 Kbps[10]。发送端每隔 5 s 发送一个窗口大小的数据,传输(N ×64) bytes,N 为滑动窗口大小。下载时间是由路灯节点定时器测得,精确到毫秒。

实验结果如表 1 所示。

表 1　路灯节点固件升级实验

代码大小/KB	滑动窗口大小	下载时间/s	代码大小/KB	滑动窗口大小	下载时间/s
5	3	124.156	5	5	123.490
10	3	251.213	10	5	248.320
15	3	374.467	15	5	365.752
20	3	496.783	20	5	488.227

通过实验可以看出:用 ZigBee 传输代码的升级效率基本上与代码大小线性相关,而滑动窗口大小对升级效率的作用不明显。

在实验过程中笔者发现,当窗口大小设为 3 时,数据基本可以在一个窗口时间内成功完成发送和应答。但当发送窗口大小变为 4 或者 5,窗口内数据会有丢帧现象,根据滑动窗口协议,丢失的帧会被选择重传,从而使升级效率变低。因此,为平衡下载效率和传输成功率,最佳的窗口大小应为 3。

5　结束语

在 LED 路灯节能系统中,路灯数量众多,分布范围广,使用传统的系统升级方法非常困难。该设计方案使用基于 ZigBee 的固件远程在线升级方法,允许节点更新其内部代码而不影响现有代码的运行,有效提高了固件升级效率,降低了设备的升级维护成本,因而具有广阔的应用前景。

本研究今后的工作重点是在多跳环境下的实验,及对升级镜像传输优化,以提高该系统的传输效率和稳定性。

参考文献(References):

[1]　李　刚,周毅波,卿柏元. 智能电力设备在线远程软件升级新方法[J]. 计算机应用,2010,30(2): 50-53.

[2]　赵　炯,贾培源,李中山,等. 嵌入式设备远程在线升级技术[J]. 计算机工程,2010,36(12): 262-264.

[3]　彭井花,蔡声镇,吴允平,等. 基于 GPRS 的嵌入式系统软件的远程在线升级[J]. 现代电子技术,2009,32(4): 47-49.

[4]　HILL J, SZEWCZYK R, WOO A, et al. System Architecture Directions for Networked Sensors [C]//Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems. New York ACM Press,2000:93-104.

[5]　STATHOPOULOS T, HEIDEMANN J, ESTRIN D. A remote code update mechanism for wireless sensor networks [R]. Los Angeles: University of California,2003.

[6]　吕志安. ZigBee 网络原理与应用开发[M]. 北京:北京航空航天大学出版社,2008.

[7]　周翔武,钱丽丽,张　冬. 基于 GPRS 数据传输终端的远程升级系统的设计[J]. 电脑知识与技术,2009,7(5): 4208-4209.

[8]　陈林林,金　朝. 一种基于嵌入式系统的远程程序更新机制[J]. 微计算机信息,2007,23(9):4-6.

[9]　杜　威,邹先霞. 基于数据流的滑动窗口机制的研究[J]. 计算机工程与设计,2005,26(11):2922-2924.

[10]　ZigBee Alliance. Network Specification[Z]. ZigBee Alliance, 2006.

[编辑:李　辉]