

文章编号:1001-9081(2010)07-1725-03

面向嵌入式无线信息终端的在线升级方法

林志雄, 鄢萍, 贺晓辉

(重庆大学 机械传动国家重点实验室, 重庆 400030)

(linzx007@gmail.com)

摘要:在深入分析国内外无线通信技术和嵌入式技术现状后,针对现有嵌入式无线信息终端软件升级方式研究的不足,以软件升级方式的快速性、安全性和可靠性为目标,提出了一种基于3G无线网络模块的软件在线方法。描述了软件在线升级方法的设计思路和工作原理,详细阐述了其关键技术的设计与实现,最后给出了应用实例和验证结果。验证结果表明,该方法升级速度快、安全系数大、可靠性高,可以有效地降低嵌入式无线信息终端软件的更新和维护成本。

关键词:车载信息终端; 嵌入式; 在线升级; 可靠性; WCDMA; 3G

中图分类号: TP311.5 文献标志码:A

Online upgrade method for embedded wireless information terminal

LIN Zhi-xiong, YAN Ping, HE Xiao-hui

(State Key Laboratory of Mechanical Transmission, Chongqing University, Chongqing 400030, China)

Abstract: Based on the existing research and achievements of wireless communication and embedded technologies home and aboard, a kind of software online upgrade method based on a 3rd generation wireless module was proposed with the goal of rapidity, safety and reliability, concerning the shortage of the existing software upgrade methods in embedded wireless information terminal. At first, the design ideas and working principles were described. Then the designs of the key technologies were expounded in detail. At last, an application case with test result was given. The result shows the method is rapid, safe and reliable, and the cost of software renewal and maintenance can be effectively reduced.

Key words: vehicle information terminal; embedded; online upgrade; reliability; Wideband Code Division Multiple Access(WCDMA); 3rd Generation (3G)

0 引言

当前,嵌入式无线信息终端软件的更新与维护主要停留在现场升级方式上,需要将设备送返开发商指定的维修网点,或由专业维护人员到达现场处理,当设备数量庞大且分布在异地时,过程繁琐而且费用昂贵。

近年来,国内外学者针对无线通信技术在嵌入式系统上的应用展开了深入的研究,其中,对硬件设计、软件架构、某种实时操作系统的采用的研究较多,取得了不少研究成果。采用无线通信技术实现软件在线升级的方式,由于不受地域限制和布线束缚,能够有效地降低软件的更新和维护成本,因此受到较为广泛的关注^[1-3]。但是,目前针对嵌入式无线信息终端软件在线升级方式的研究大多只停留在升级方式的设计上,缺乏针对升级方式的快速性、安全性和可靠性等目标进行充分的研究。

因此,本文针对已有研究的不足,综合考虑现有无线通信技术和嵌入式软硬件技术,研究一种面向嵌入式无线信息终端的快速、安全且可靠的软件在线升级方法。

1 设计思路和工作原理

1.1 软件在线升级方法的设计思路

2009年1月7日,中国工业和信息化部同时发放了

WCDMA、CDMA2000 和 TD-SCDMA 三张 3G 牌照,标志着我国正式进入第三代移动通信时代。3G 是将无线通信与互联网等多媒体通信结合的新一代移动通信系统,可以实现全球漫游,具有强大的多用户管理功能、保密性和服务质量,在室内、室外和行车环境中分别能支持至少 2 Mbps、384 Kbps 和 144 Kbps 的传输速度,较之 GSM、GPRS 有了很大的提高^[4]。因此,在嵌入式无线信息终端上使用 3G 无线网络模块,为实现软件的快速升级提供了一个可靠的平台。

嵌入式软件在线升级方式的可靠性主要受两个因素的影响:一个是待升级软件更新数据远程传输的可靠性,另一个是软件升级后系统重新启动的可靠性^[5]。WCDMA 网络在 GSM、GPRS 的基础上,采用双向身份认证,增加了安全密钥长度和网内、网间的安全认证机制,因此能够安全、可靠地传输更新数据。同时,为了提高软件在线升级的速度和成功率,可在网络应用层添加断点续传功能加以保证。在 Windows CE、Vxworks、Linux 等嵌入式实时操作系统中,一般设计一个独立的 Bootloader 程序,用来初始化硬件设备、建立内存空间的映射图,从而将系统的软硬件环境带到一个合适的状态,以便为最终调用操作系统内核准备好正确的环境^[6]。因此,软件升级后系统重新启动的可靠性与 Bootloader 程序的设计紧密相关。

1.2 软件在线升级方法的工作原理

依据上述分析,本文设计了如下方案。无线信息终端通

收稿日期:2010-01-22;修回日期:2010-03-04。

基金项目:国家自然科学基金资助项目(50775228);重庆市自然科学基金资助项目(CSTC2006BB2237)。

作者简介:林志雄(1985-),男,福建莆田人,硕士研究生,主要研究方向:嵌入式系统; 鄢萍(1967-),女,四川内江人,教授,博士生导师,主要研究方向:机电一体化、网络化制造; 贺晓辉(1978-),男,河北人,博士研究生,主要研究方向:网络化制造、嵌入式系统。

过 3G 无线网络模块连接到 WCDMA 移动通信系统,进而接入 Internet。远程服务器采用有线方式与 Internet 连接,与终端之间进行基于 TCP/IP 协议的信息交互。远程服务器持有各软件的最新版本,待升级软件的更新数据经过 Internet 传输到无线信息终端。

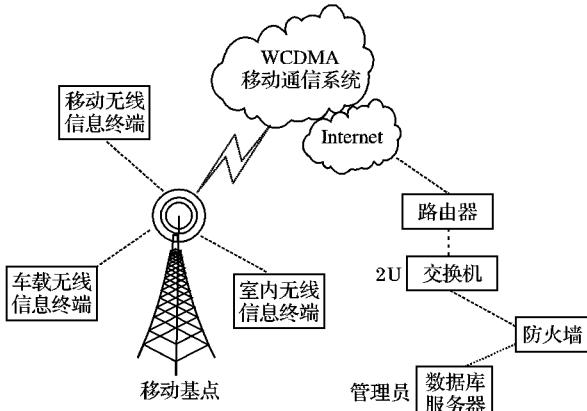


图 1 系统工作原理

软件在线升级方法采用标准的客户端/服务器模式。远程服务器的数据库记录了各无线信息终端的序列号、密码和当前各软件的版本信息。服务器端程序监听并接受可信用户的连接请求。客户端与服务器的监听端口建立连接,发送本机序列号和密码进行登录请求,在通过服务器的身份验证后,发送本机当前各软件版本配置信息,然后循环等待软件升级通知。服务器检验并记录联机无线信息终端需要升级的软件版本,然后向客户端发送待升级软件列表。客户端得到用户的授权后进入软件在线升级模块。服务器创建软件下载子进程,允许客户端下载指定软件版本到无线信息终端,最后释放软件下载子进程,继续监听新用户的连接请求。

2 关键技术的设计与实现

2.1 基于 WCDMA 实现软件在线升级模块

2.1.1 软件在线升级方法的优化设计

嵌入式无线信息终端的软件按功能分为应用软件和系统镜像两部分。应用软件的升级比较简单,只需在待升级软件下载完毕后,先卸载旧版本软件,再装载新版本软件即可。嵌入式系统中,系统镜像传统的升级方法通常是从远程服务器下载整个镜像文件到本地路径,然后重启系统通过 Bootloader 程序实现。该方法通常需要下载几十兆大小的文件,如果由无线网络实现,耗时将会太长,因此不适用于无线信息终端。为此,本文重新设计一种系统镜像的升级方法。在无线信息终端的软件配置文件中,不仅要记录各应用软件的版本信息,而且要记录当前硬件平台各驱动的版本信息。服务器对无线信息终端和远程服务器两端的镜像文件中各硬件驱动的版本信息进行比较,当需要升级系统镜像时,客户端在线升级模块只下载需要升级的驱动文件到本地路径,然后修改本机软件版本配置文件,最后重新启动系统,根据配置文件的修改记录,装载最新版本的硬件驱动即可。与传统的升级方法相比,本方法需要下载的文件数目明显减少,升级速度必然提高。

2.1.2 软件在线升级模块的实现

软件在线升级模块采用 PUSH 策略^[7],服务器作为软件在线升级任务的主动发起者和组织者,检测并记录无线信息终端需要升级的所有软件的版本信息,最后采用批处理方式传输待升级软件的更新数据。

服务器首先将待升级软件拆分成多个固定长度的数据单元,然后以数据单元为核心封装成数据包。如表 1 所示,数据包的格式含包头标志、终端 ID、总包数、包序号、包长度、数据单元、校验码和包尾标志,总长度规定为 512 个字节。服务器依次发送所有数据包,客户端开辟数据缓存,接收每个数据包,并根据数据包格式进行数据解析和容错校验,然后向服务器返回确认信息。服务器将根据该确认信息判断是否需要重新发送前一个数据包。客户端成功接收完 COUNT 个数据包后,向服务器发送下载成功的确认消息,否则发送下载失败的确认消息,并等待下次软件升级。服务器根据客户端回复的消息,将此次升级过程详细信息写入数据库。

表 1 数据包格式

内容	格式	字节数	内容	格式	字节数
包头	SOI	2	包长度	LENGTH	2
终端 ID	VITID	4	数据单元	INFO	LENGTH
总包数	COUNT	2	校验码	CRC	4
包序号	NUMBER	2	包尾	EOI	2

更新数据传输完毕后,开始进行软件升级。如果待升级软件是硬件驱动文件,则需要重启系统,通过 Bootloader 程序实现相应操作,该部分具体流程将在后续章节中介绍;如果待升级软件是应用软件,客户端首先取得该应用软件的主窗口句柄,然后向主窗口发送关闭消息,并不断探测该窗口句柄,直到此句柄失效(表明旧版本应用软件已结束运行),此时将旧版本应用软件按指定格式重命名,再剪切到备份路径,最后拷贝新版本软件到旧版本软件原来路径后调用执行。如果同时有多个应用软件要进行升级,则按照服务器上待升级软件的批处理顺序,依次进行上述操作。客户端完成软件升级后,将修改无线信息终端上指定路径下的本机当前各软件版本配置文件的内容,包括当前运行的软件版本号、历史运行的软件版本号、旧版本软件的备份路径、最近一次软件在线升级的日期等信息。

2.2 断点续传功能的实现

软件在下载过程中,极有可能因为出现网络阻塞、系统意外断电等原因,造成软件未能一次下载完毕。如果每次都重新开始下载,势必速度缓慢、效率低下,为此本方法在更新数据的远程传输过程中添加断点续传功能。客户端在无线信息终端上指定路径下创建一个软件传输记录文件,对传输中断的软件进行记录,包括软件的名称、大小、传送时间、已传字节数等内容。客户端每次进入在线升级模块后,首先读取软件传输记录文件信息。如果存在未下载完毕的待升级软件,则向服务器发送重发文件请求。服务器收到该请求后,创建软件下载子进程,根据客户端发送的文件名和已接收字节数,打开本地存储路径下对应文件,并将文件指针定位到相应字节处,然后读取一个数据包的字节数后开始数据传输。如果已下载包数为 N 个,则从第(N+1)个数据包开始下载,直到下载完 COUNT 个包。断点续传功能可以节省网络资源,降低操作系统的运行成本,提高软件在线升级的速度和成功率。

2.3 软件在线升级后系统重新启动的可靠性设计

嵌入式操作系统中,通常将 Bootloader 程序和系统镜像保存在非易失性存储介质上。考虑到 NAND Flash 在使用过程中可能产生坏块或位反转现象而造成数据损坏,而且用户误操作等原因也可能造成系统崩溃,为确保系统启动的可靠性,本方法同时选择 NOR Flash 和 NAND Flash 两种非易失性

存储介质,并在Bootloader程序中设计系统镜像的备份和一键恢复机制。其中,NOR Flash用于存储Bootloader程序,NAND Flash划分为3个分区:第1个分区用于存储默认运行的系统镜像,命名为运行区;第2个分区用于存储系统镜像的备份,命名为备份区;第3个分区在系统启动后模拟硬盘,用于存储本机当前各软件版本配置文件、各种应用软件、软件传输记录文件、待升级硬件驱动文件等,命名为模拟区。

2.3.1 系统启动流程设计

无线信息终端上电后,跳转到Bootloader程序起始地址执行,完成硬件的初始化,并读取控制面板按键状态执行相应的功能模块,按键扫描程序超时则直接启动系统。系统启动的流程表如图2所示。

其中,箭头1表示从运行区拷贝系统镜像到内存;箭头2表示从内存拷贝系统镜像到备份区;箭头3表示从备份区拷贝系统镜像到内存;箭头4表

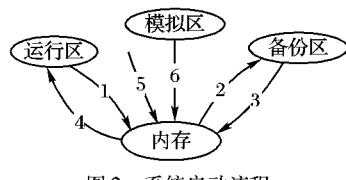


图2 系统启动流程

示从内存拷贝系统镜像到运行区;箭头5表示跳转到内存中镜像文件起始地址开始执行,并在系统启动后自动运行指定应用软件;箭头6表示根据本机软件版本配置文件中硬件驱动版本的修改记录,卸载该硬件模块的旧版本驱动,并从模拟区指定路径下加载新版本驱动文件。

系统直接启动过程为1→5;系统镜像升级过程为1→5→6;系统镜像备份过程为1→2→5;系统镜像恢复过程为3→4→5。

2.3.2 系统启动的可靠性设计

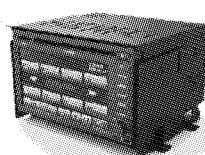
为了确保NAND Flash存在的坏块和位反转现象不会造成系统瘫痪,需要在Bootloader中添加对NAND Flash的坏块识别和数据读写纠错功能。

Bootloader程序首先对整块NAND Flash进行坏块扫描,创建并更新坏块地址表,这样在对Flash进行擦除和写入操作时可以直接跳过这些坏块。在NAND Flash出厂前,厂商已将其固有坏块的Page1的Spare Area的第6个字节标记为不等于0xff的值。使用过程中利用错误检查与修正(Error Checking and Correction,ECC)算法进行数据纠错。ECC算法可通过硬件或软件实现,ARM7以上的处理器都带有硬件ECC检测功能,MIPS系列处理需要通过软件实现。ECC算法将每256字节的原始数据生成3字节的ECC校验和:6位列校验码,16位行校验码,剩余2位置1。Bootloader程序向Flash写入数据时,由每256字节生成一个原始的ECC校验和,保存到该Page的带外数据(Out-Of-Band,OOB)数据区中。当从Flash读数据时,由每256字节生成一个新的ECC校验和,然后与原始ECC校验和做按位异或运算。运算结果如果为0,则表明数据读写未出错;如果存在11个位的值为1,则表明有1位错误且通过算法纠正;如果只存在1个位的值为1,则表示OOB数据出错,需要重写OOB数据区内容;其他情况均表示出现了无法纠正的错误,此时该Page所在的Block需作为坏块处理。为了和生产过程中产生的坏块的记录信息保持一致,Bootloader程序也将新坏块的Page1的Spare Area的第6个字节处标记为非0xff的值,并更新坏块地址列表。

3 应用实例

本方法已应用到国内某车载无线信息终端中,并取得了良好的效果,图3展示了该终端的外观。该终端选用基于

MIPS32的高性能、低功耗的RMI AU1250处理器,主频可达600 MHz,提供了USB 2.0、AC97、UART等丰富的外部接口^[8]。数据传输采用基于USB 2.0接口的SIM5128 3G无线网络模块,支持下行速率为7.2 Mbps和上行速率为5.76 Mbps的高速数据传输服务^[9]。NAND Flash选用三星公司的K9K1G08U0M芯片,提供128 M×8 bit(1 Gbit)的存储空间,支持整页读写、块擦除、多页读取和回写等操作模式,并支持ECC坏块检测和校验^[10]。整个平台以AU1250为核心,搭建Windows CE实时操作系统,具有独立设计的Bootloader程序。软件开发工具采用功能强大的Visual Studio 2005,开发语言为面向对象的VC++ .NET精简框架集。



无线信息终端系统启动后,客户端程序调用Windows CE自带的自动拨号功能,根据默认配置连接远程服务器,然后发送保存在NAND Flash第3个分区的序列号、密码和本机当前各软件版本配置信息,

并在后台等待远程服务器发送软件升级通知。软件升级过程中,若WCDMA信号较好,升级速度很快;若WCDMA信号较差,升级速度稍慢;若中途不慎掉电造成传输中断,断点续传功能保证了升级过程的顺利进行。

4 结语

本文提出的嵌入式无线信息终端软件在线升级方法,通过采用3G无线网络模块,摆脱了地域限制和布线束缚,提高了软件在线升级的快速性和便捷性;通过重新设计系统镜像的升级方法和在网络应用层添加断点续传功能,提高了软件在线升级的速度和成功率;通过在Bootloader程序中实现系统的备份和一键恢复功能,以及对NAND Flash的可靠性设计,提高了软件在线升级的安全性。该方法集快速性、安全性和可靠性于一体,有效地降低了嵌入式无线信息终端软件的更新和维护成本,具有广阔的应用前景。

参考文献:

- [1] van ROOVEN R M, CRAWFORD K E. Method and system for fail-safe recovery and upgrade of an embedded operating system [EB/OL]. [2009-08-20]. <http://www.freepatentsonline.com/6591376.html>
- [2] 陈琦,丁天怀,李成,等.基于GPRS/GSM的低功耗无线远程测控终端设计[J].清华大学学报:自然科学版,2009,49(2):223-225,231.
- [3] 农毅.基于CAN总线和GRPS的无线车载数据传输[J].计算机工程,2008,34(18):239-242,245.
- [4] 孙迪.基于Windows CE系统的WCDMA协议安全性研究与实现[D].天津:天津大学,2007.
- [5] 王恒,王颖,王泉,等.基于Bootloader的可靠嵌入式软件远程更新机制[J].嵌入式软件应用,2007,23(7):57-59.
- [6] 李毅,李连云,张伟宏,等.Bootloader面向不同结构Flash的实现[J].计算机工程,2008,34(4):82-83,86.
- [7] 王子健,张军,罗喜伶.基于TFFS的嵌入式系统在线升级设计与实现[J].计算机工程,2006,32(13):257-259.
- [8] RMI. RMI Alchemy Au1250 processor data book [EB/OL]. [2009-08-25]. <http://www.rmicorp.com/products/Au1250.htm>
- [9] SIM5128 Plus(PCBA) [EB/OL]. [2009-09-25]. <http://www.sim.com/wm/cn/wm/html/en/AS/ProductDetail.aspx?id=87>
- [10] K9K1G08U0M-YCBO flash memory [EB/OL]. [2009-08-30]. http://www.datasheetcatalog.org/datasheets/480/265074_DS.pdf