无线传感器网络远程重编程研究与实现

闫晓晓,杨 冬,董 平
(北京交通大学 电子信息工程学院,北京 100044)

摘 要:无线传感器网络是由大量节点和网关设备组成的,节点和网关的分布范围非常广泛,有时它们可能被分布在人迹罕至的恶劣环境中。根据应用需求,经常需要对节点和网关的软件进行更新或替换,鉴于其分布环境问题,每次将设备回收进行软件更新很不现实,因此考虑对无线传感器网络进行远程重编程。在对无线传感器网络和下一代互联网研究的基础上,文中主要对无线传感器网络重编程的关键技术进行了研究,在现有 Contiki loader 模块的基础上,搭建通信操作平台并实现了基于 Contiki 的无线传感器网络重编程,实现中心管理服务器对无线传感器节点的远程重编程。

关键词:无线传感器网络;Contiki 操作系统;重编程;ELF 文件
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2013)02-0019-04
doi:10.3969/j.jssn.1673-2013.01.005

Research and Implementation of Remote Reprogramming of Wireless Sensor Networks

YAN Xiao-xiao, YANG Dong, DONG Ping
(School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: Wireless sensor network is composed by a large number of nodes and gateways, these nodes and gateways are distributed widely, sometimes they may be distributed in the harsh inaccessible environment. According to the application requirements, need to update or replace their software, in view of the distribution of environmental issues, each device recovery software update is not realistic, and therefore consider reprogramming wireless sensor networks remotely. Based on the research of wireless sensor networks and the next generation of Internet research, in this paper, the key technology of the reprogramming of wireless sensor network is analyzed. On the basis of the existing the Contiki loader module, build a communication platform, and a kind of reprogramming system based on Contiki runtime loading module is implemented. In this method, the central management server can reprogrammed the wireless sensor nodes remotely.

Key words: wireless sensor network; Contiki operation system; reprogrammimg; ELF

0 引 言

随着小型化、低成本的电子电器技术的发展,无线传感器网络的应用越来越广泛,包括战场监控、工业控制、生态管理、健康监测等。无线传感器网络包含一系列可编程嵌入式系统,其行为由节点内的软件决定,在添加新的应用和增添服务功能的时候,设备的远程重编程操作很有必要。但是有限的能量供应、恶劣的工作环境、有限的硬件存储资源使无线传感器网络重编程面临着重大的挑战。

收稿日期:2012-05-22;**修回日期**:2012-08-25
基金项目:"新一代宽带无线移动通信网"国家科技重大专项(2012ZX03005003);国家自然科学基金资助项目(60870015,61100217,61100219)
作者简介:闫晓晓(1987-),女,硕士研究生,研究方向为无线传感器网络;董 平,博士,讲师,研究方向为通信网络体系结构、新一代移动互联网技术。

1 无线传感器网络的重编程方法

无线传感器网络[1]的重编程是一个十分活跃的研究领域,其研究方向主要分为分发策略和重编程机制两个方面。分发策略用于在已部署好的网络中高效、节能地传输数据,重编程机制又可以分为系统化重编程、虚拟机和模块化重编程等。目前无线传感器网络重编程的方法主要有系统化重编程[2]、基于虚拟机[3]的重编程和模块化重编程。

1.1 系统化重编程

在系统化重编程中,现有的软件完全被更新的系统替代。更新的系统存储在外部存储器中,在系统重启时被拷贝到内部存储器中。系统化重编程简单、可靠,由于是完全网络的重编程,所以开发者不需要担心错误的数据接入、跳转和加载。但是系统化重编程也有一些缺点。即使只需要更新一小部分代码,系统化重编程也必须更新整个系统,这样就需要更多的能量、时间并占用更多的内存空间,影响工作效率。目前使

用系统化更新的操作系统主要有 TinyOS[4] 和 Nano-RK。

1.2 基于虚拟机的重编程

在基于虚拟机的无线传感器网络中,每个节点运行的都是一个虚拟机的实例。虚拟机用来执行网络数据包和字节指令。Mate 是基于 TinyOS 的第一个 WSN 虚拟机。Mate 接收命名为 capsule 的网络数据包指令。一个长度为 23 字节的 capsule 网络数据包包含需要更新的代码或补丁。基于虚拟机的重编程对处理时间和 CPU 的处理能力要求较高,且只适用于少数优先级较高的指令。

1.3 模块化重编程

在模块化重编程[5]中,运行的操作系统将系统内核与可编程加载模块分离开来。内核模块不能被更改,可编程加载模块中所有的应用程序和服务提供程序都可以被动态加载或替换。模块化重编程只需根据需求更改某些模块,而无需更新整个操作系统,这样有利于节省更多的能量、时间和内存空间,有利于提高工作效率。综合来看,模块化重编程更适合于无线传感器网络的应用需求。而 Contiki 就是一个典型的使用模块化重编程的操作系统。

2 Contiki 操作系统

2.1 Contiki 操作系统简介

Contiki[6,7]是一个可移植性高、基于多线程的事件驱动型操作系统,支持原型进程以及可选的抢占式多任务,它是第一个支持模块化更新的操作系统。Contiki 运行时 RAM 和 ROM 内核中都存在可加载程序模块,该模块可以实现对某些程序的动态加载、卸载操作,如图 1 所示。

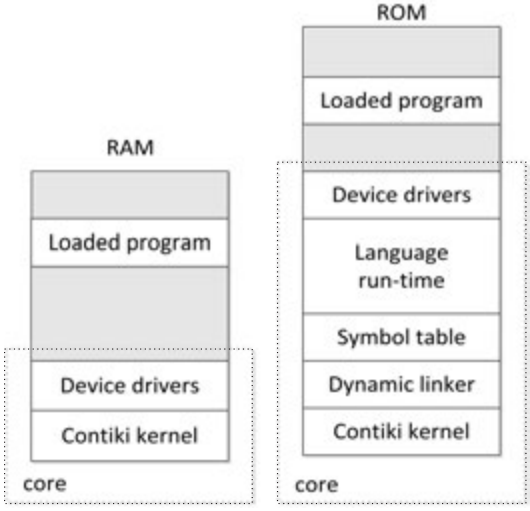

图 1 RAM 和 ROM 中内核和可加载模块

Contiki 内核对于所有事件的处理都是基于同一个优先级的,并不存在事件抢占问题[8],事件只能被中断抢占。内核是一个不可重编译的模块,Contiki 对于内核、程序加载模块、符号表和通信接口的更改都是不支持的。而其他模块,如文件系统、shell 脚本应用、能量管理模块等则都是可以被动态加载和重编译的。可编程程序是通过动态重新安置函数和包含重新安置信息的二进制文件实现的。当一个程序被加载到系统中时,装载器首先依据二进制文件提供的信息给程序提供足够的存储空间。如果存储空间不够,程序加载将失败。在程序下载完成后,装载器调用程序初始化函数。初始化函数将会开启或替换进程。

2.2 重编程进程处理

一个正在运行的操作系统包括内核、库、程序加载器和进程,如图 2 所示。其中,Loadable 部分代表可加载模块,包括应用程序和服务;Core 部分代表 Contiki 系统一旦运行起来,不可更改的模块;硬件资源部分代表 Contiki 系统运行时需要的硬件及驱动模块。在 Contiki 中,服务就是一个可以被其他进程应用的进程,它可能以共享库的形式存在。一个服务可能被不止一个应用程序使用。和所有应用进程一样,服务也可以在运行的 Contiki 系统中动态地加载和更替[9]。每一个服务进程都有一个服务 ID,当服务进程被替换的时候,服务 ID 会被保留。内核提供一个特殊的机制用于更换进程并保留进程 ID。当服务被更换的时候,内核通过给运行的服务进程发送一个特殊的事件通知该服务进程。进程收到通告事件,就退出系统。许多服务都有一个转换到新进程的中间状态。内核给新的服务进程分配一个指针,服务给新进程分配一个状态描述符。存放状态描述符的内存空间必须是一个共享内存,这样做是为了保留进程 ID,因为当旧的进程被删除的时候,其内存空间会被释放,所以进程 ID 不能被保留在进程占用的内存空间中。

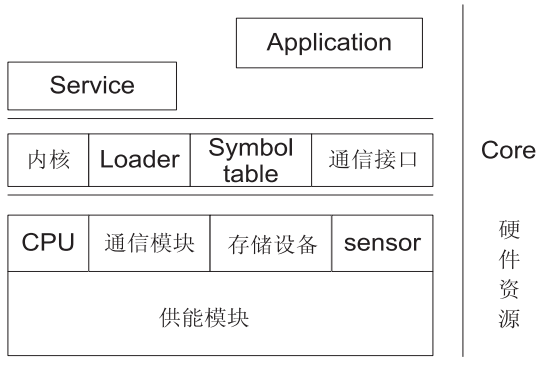

图 2 运行时的 Contiki 体系架构

2.3 可加载模块

Contiki 支持模块的重编程。通常通过网络或者 EEPROM 获取模块,由于 Contiki 支持模块加载机制,所以它可以实现动态加载或更新软件。

Contiki 系统产生的可执行文件符合 ELF[10]格式,

可加载模块采用的是可重定位的 ELF 文件,该种文件是编译但未链接的二进制文件。ELF 文件中存在某些无法解析的函数名或变量名,在 ELF 文件中,某些函数名或变量名的引用地址是空白的,需要通过链接过程解析这些函数名或变量名。链接过程可以在加载前或加载时进行。ELF 文件包含所有的可重新安置信息,即模块大小和所在内存位置。另外,该重新安置信息也用来更新符号表。为了体现更大的灵活性,这些模块设计为松耦合方式,模块间通过内核进行通信。这些设计使得模块化重编程更加灵活。Contiki 也支持动态的链接[11]和装载[12],这对于支持模块化重编程也是一个非常重要的特点。

3　Contiki 中重编程的实现

Contiki 系统中支持重编程的文件符合 ELF 格式,该格式的文件可以在系统运行时被动态的链接、重定位和加载[13]。

3.1　ELF 文件

ELF 文件——一种常用的二进制可执行链接格式文件。随着对 Linux 嵌入式系统开发的不断深入,越来越多的 ELF 文件被应用在嵌入式平台上。ELF 文件可分为可重定位文件、可行性文件、共享 ELF 文件。Contiki 中典型的 ELF 文件的结构如图 3 所示。

图 3　ELF 文件基本格式

ELF 头部——ELF 文件头部位于文件开头处,并且反应整个文件的组织形式。段保存用于连接的目标文件信息如指令、数据、符号表、重定位信息等。

text——代码段。

data——数据段。

符号表——保存源代码中用到的变量和函数,这些变量和函数都可以称为符号。

字符串表——用于存放 ELF 文件的段名、变量名。

节头表——节头表是 ELF 文件中除了文件头以外最重要的结构,它描述各个节的信息,如节名、节的长度、在文件中的偏移、读写权限及节的其他属性。也就是说,ELF 文件的节结构就是由段表决定的,编译器、链接器和装载器都是依靠段表来定位和访问各个段的属性的。

重定位表—— ELF 文件中有个重定位表用来专门保存于重定位相关的信息,它在 ELF 文件中往往是一个或多个段。每个可重定位的 ELF 文件都有重定位表,用于描述如何修改相应的段里的内容。一个重定位表往往就是 ELF 文件中的一个段,因此重定位表又称重定位段。

3.2　重编程实现过程

基于 Contiki 的重编程[14]的实现过程主要分为中心服务器端和节点端两部分。中心服务器端负责源程序的编译,将源程序编译生成 ELF 格式的. o 文件,那些支持可重定位的. o 文件即可被重编程。节点端接收到. o 文件后,通过 Contiki 系统中的 loader 模块,对其进行处理,实现对. o 文件的重定位与加载运行。重编程的数据流分发过程如图 4 所示。

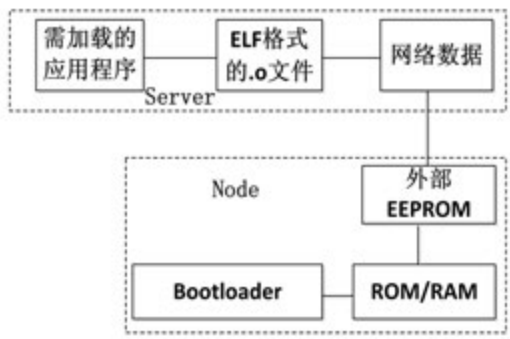

图 4　数据流的存储分发过程

本实验中,首先在中心服务器和待加载节点之间建立 TCP 连接,在中心服务器端通过套接口发送 ELF 格式的. o 文件,由于 Contiki 支持套接口通信,在待加载的节点端只需监听特定的 TCP 端口,即可接收由中心服务器端发送的. o 文件。

具体实现步骤如下:

(1)中心服务器编译生成一个 Contiki core,并通过烧写器将其加载到节点。网络中的所有节点都必须运行同一个 Contiki core。

(2)去除烧写器,在节点与中心服务器之间通过网关建立 TCP 连接。

(3)中心服务器发送. o 文件给节点,节点上的 Contiki loader 模块加载. o 文件并将其转化为适合 Contiki 的 process,进而运行 process,实现对系统服务及应用程序的加载或更替。

Contiki 中 loader 模块对于. o 文件处理时所用到的系统函数及变量指针见表 1。

运行 Contiki 的节点 loader 模块对于接收到的 ELF 格式的. o 文件主要做以下处理。节点首先将收到的. o 文件存入 EEPROM 中的 EEPROMFS _ ADDR _

CODEPROP 区域。新的. o 文件加载前,调用 elfloader_unload( ) 函数卸载 elfloader_loaded_process 指针指向的进程或服务,清空 elfloader_loaded_process 指针区域。然后调用 elfloader_load( ) 函数加载 EEPROMFS_ADDR_CODEPROP 区域中的. o 文件。

表 1 Contiki loader 模块中各系统函数及变量指针

系统函数及变量指针	功能
EEPROMFS_ADDR_CODEPROP	指定. o 文件存放在 EEPROM 中的位置
elfloader_loaded_process	指向已加载、未运行完毕的 process
elfloader_unload( )	清空 elfloader_loaded_process 指针区域
elfloader_load( )	加载 EEPROM 中存放的. o 文件
relocate_section( )	重定位 ELF 文件中各 section 内容
elfloader_arch_write_rom( )	将. text 和. rodata 写进 ROM 指定位置
seek_read( )	将. data 段写入 RAM 指定位置

elfloader_load( ) 函数主要负责处理. o 文件。首先处理. o 文件头部,通常使用一个兼容的 ELF 格式的文件头部。ELF 格式的文件中不同的节包含不同的数据信息,所以在数据链接、加载阶段应分节处理。首先对. text、. data、. rodata 节进行重定位链接,然后用 relocate_section( ) 函数对每节内容进行重定位操作。通过 elfloader_arch_write_rom( ) 函数将. text 和. rodata 节写入 ROM 指定位置,通过 seek_read( ) 函数将. data 节写入 RAM 指定位置。CPU 为每节分配 ROM 或 RAM 地址。最后将处理后的. o 文件进程化,给每个进程分配一个进程 ID,等待 CPU 处理。

3.3 实验测试

设计方案确定后,需要对方案进行硬件实施,并测试其实验结果。以运行支持 IPv6 和 6lowpan 的 Contiki 系统的节点作为普通节点。以具有以太网接口的 PC 机作为中心服务器,以具有 802.15.4 接口和以太网接口的 ARM 板作为网关。中心服务器端通过 TCP 给运行 Contiki 的节点发送. o 文件,节点接收、重定位并运行. o 文件,最终实现中心控制服务器对节点的远程重编程。方案实际部署如图 5 所示。

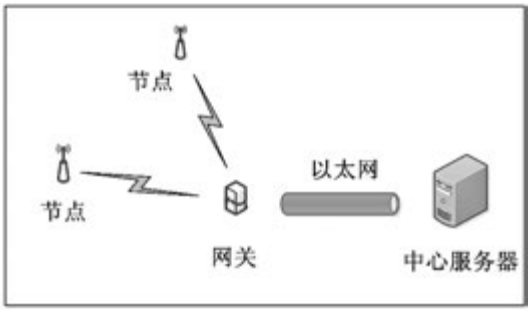

图 5 系统测试环境

由于方案实施时,中心控制服务器、网关和节点的地址都支持 IPv6 和 6lowpan,所以对实验设备的地址配置情况如下:节点地址为 fe80::11:22ff:fe33:4455;网关地址为 fe80::1/64;中心服务器地址为 fe80::11:22ff:fe33::2020。

实验结果:中心服务器给节点烧写 Contiki core,使得节点运行 Contiki 系统。节点通过网关与中心服务器建立 TCP 连接。此时,在中心服务器端通过网关给节点传送需要加载的控制节点亮灯的 led. o 文件,节点接收到 led. o 文件后,通过 loader 模块加载处理,最后点亮节点上相应的指示灯。

4 结束语

无线传感器网络的重编程是有效克服无线传感器网络能量和硬件资源有限等缺点不可或缺的技术。鉴于无线传感器网络的重编程需求,在 Contiki 系统现有 loader 模块的基础上,搭建通信环境,实现了对无线传感器网络的重编程。以达到在不改变节点物理位置、不影响节点工作的情况下,仅通过中心服务器更改节点的应用及配置信息。

在该设计研究的基础上,后续可以根据实际应用需求加载应用程序,或更改除 Contiki kernel 以外的系统配置。这样更有利于对无线传感器网络的远程管理和配置。

参考文献:

[1] 孙利民,李建中,陈 渝,等. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[2] Bhatti S,Carlson J,Dai Hui,et al. MANTIS OS:An Embedded Multithreaded Operating System for Wireless Micro Sensor Platforms[J]. Mobile Networks and Applications,2005,10(4):563-579.

[3] Müller R,Alonso G,Kossmann D. A virtual machine for sensor networks[J]. ACM SIGOPS Operating Systems Review,2007,41(3):145-158.

[4] Levis P,Madden S,Gay D. The emergence of networking abstractions and techniques in TinyOS[C]//Proceedings of the 1st Conference on Symposium on Networked Systems Design and Implementation. USA:USENIX Association,2004.

[5] Shafi N B. Efficient Over-the-air Remote Reprogramming of Wireless Sensor Networks[D]. Canada:Queen's University,2011.

[6] Dunkels A, Gronvall B, Voigt T. Contiki-a lightweight and flexible operating system for tiny networked sensors[C]//29th Annual IEEE International Conference on Local Computer Networks. France:IEEE,2004:455-462.

[7] Dunkels A,Schmidt O,Voigt T,et al. Protothreads:simplifying event-driven programming of memory-constrained embedded systems[C]//Proceedings of the 4th International Conference on Embedded Networked Sensor Systems. USA:ACM,2006:29-42.

(下转第 27 页)

评价模型有效地改善了现有 GSM 网络频点分布问题,成功地避免了同、邻频信号对 GSM 网络的干扰,达到优化 GSM 网络性能的最终目的。

参考文献:

[1] 戴美泰,吴志忠,邵世祥,等. GSM 移动通信网络优化[M]. 北京:人民邮电出版社,2003.

[2] Harte L, Bromley B, David M. Introduction to GSM: Physical Channels, Logical Channels, Network Functions, and Operation [M]. [s. l.]: ALTHOS, 2008.

[3] Ali S Z. A heuristic decomposition methodology for channel assignment problems in mobile communication systems[C]// The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. [s. l.]: [s. n.], 2002: 2175-2179.

[4] Nsivarajan K, Meelieee R J, Ketehum J W. Channel assignment in cellular radio[C]//Proc. of 39th IEEE Veh. Tech. Conf. . [s. l.]: [s. n.], 1989: 846-850.

[5] Sung C W, Wong W S. A graph theoretic approach to the channel assignment problem in cellular systems[C]//IEEE Veh. Tech. Conf. . [s. l.]: [s. n.], 1995: 604-608.

[6] Ali S Z. A Graph - theoretic Decomposition Technique for Fixed Channel Assignment Problems in Cellular Radio Networks[C]//IEEE Veh. Tech. Conf. . [s. l.]: [s. n.], 2002: 1064-1068.

[7] Even G, Lotker Z, Ron D, et al. Conflict-free colorings of simple geometric regions with applications to frequency assignment in cellular networks[C]//Proc. of the 43rd Annual IEEE Symposium on Foundations of Computer Science. [s. l.]: [s. n.], 2002: 691-700.

[8] Funabiki N, Takefuji Y. A Neural Network Parallel Algorithm for Channel Assignment Problems in Cellular Radio Networks [J]. IEEE Trans. on Veh. Tech. , 1992, 41: 430-437.

[9] Berger M O. Neural channel assignment - the fast way[C]// Proc. of IEEE International Conf. on Neural Networks. [s. l.]: [s. n.], 2002: 1557-1560.

[10] Smith K, Palaniswami M. Static and dynamic channel assignment using neural networks[J]. IEEE Journal on Selected Areas in Communications, 1997, 15(2): 238-249.

[11] Hanamitsu A, Ohta M. A maximum neural network with self-feedbacks for channel assignment in cellular mobile systems [C]//IJCNN'02. [s. l.]: [s. n.], 2002: 2814-2818.

[12] Poli R. A Field Guide to Genetic Programming[M]. UK: Lulu Enterprises, 2008.

[13] Alabau M, Idoumghar L, Sehott R. New Hybrid Genetic Algorithm for the Frequeney Assignment Problem[C]//Proc. of the 13th International Conf on Tools with Artificial Intelligence. [s. l.]: [s. n.], 2001: 136-142.

[14] Ghosh S C, Sinha B P, Das N. Channel assignment using genetic algorithm based on geometric symmetry [J]. IEEE Trans. on Veh. Tech. , 2003, 52(4): 860-875.

[15] Yoshino J, Ohtomo I. Efficient channel assignment using the genetic algorithm in the cellular mobile communication system [C]//The 5th International Symposium on Wireless Personal Multimedia Communications. [s. l.]: [s. n.], 2002: 636 - 639.

[16] Haider B, Zafrullah M, Islam M K. Radio frequency optimization & quality of service evaluation in operational GSM network[C]//Proceedings of the world Congress on Engineering and Computer Science. [s. l.]: [s. n.], 2009: 1-4.

[17] 成　曦. 浅谈 GSM 无线网络优化[J]. 电信技术, 2003(5): 71-73.

[18] 郑　磊. GSM 网络优化研究[J]. 科技创新导报, 2009 (24): 22-22.

[19] John S N, Okonigene R E, Akinade B A. Optimized Remote Network Using Specified Factors as Key Performance Indices [J]. Global Journal of Computer Science and Technology, 2010, 10(5): 14-17.

[20] 玄光男,程润伟. 遗传算法与工程优化[M]. 北京:清华大学出版社,2004.

(上接第 22 页)

[8] Krohn M, Kohler E, Kaashoek M F. Events can make sense [C]//Proceedings of the USENIX Annual Technical Conference. USA: USENIX Association, 2007.

[9] Dunkels A, Finne N, Eriksson J, et al. Run-time dynamic linking for reprogramming wireless sensor networks[C]//Proceedings of the Fourth ACM Conference on Embedded Networked Sensor Systems (SenSys). USA: ACM, 2006: 15-28.

[10] Levine J R. Linkers and loaders[J]. ACM Computing Surveys (CSUR), 1972, 4(3): 149-167.

[11] Polastre J, HuiJ, Levis P, et al. A unifying link abstraction for wireless sensor networks[C]//Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems. USA: ACM, 2005: 76-89.

[12] Low C P, Fang C, Ng J M, et al. Load-balanced clustering of wireless sensor networks[C]//ICC '03. [s. l.]: [s. n.], 2003: 750-759.

[13] 孟硕培. 无线传感器网络节点重编程研究与设计[D]. 杭州:浙江大学,2008.

[14] Dunkels A. The Contiki Operating System[EB/OL]. 2006. http://www. sics. se/adam/contiki.

无线传感器网络远程重编程研究与实现

作者： 闫晓晓， 杨冬， 董平
作者单位： 北京交通大学 电子信息工程学院,北京 100044
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(2)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjfz201302007.aspx