文章编号:1001 - 9081(2007)02 - 0278 - 04

一种基于 lwIP 的 CAN/Ethernet 嵌入式网关设计

张文亚[1,2],李 恩[1,2],蔡 丽[1,2],梁自泽[1]
(1. 中国科学院 自动化研究所,北京 100080; 2. 中国科学院 研究生院,北京 100049)
(wenya. zhang@ ia. ac. cn)

摘 要:为了实现控制中心的以太网和生产现场 CAN 总线的互联,完成对生产现场的实时监控,设计了 CAN/Ethernet 嵌入式网关。通过移植轻量级的 TCP/IP 协议栈(lwIP)实现了以太网通信所需的 TCP/IP 协议栈,通过对 CAN2.0B 数据扩展帧报文标志符的重定义提出并实现了 CAN 应用层协议,提出了一种转换协议来完成两种协议的转换和对通信的控制,实现了 CAN 节点和以太网服务器及不同网关下 CAN 节点之间的通信。

关键词:CAN 总线;以太网;网关;轻量级的 TCP/IP 协议栈
中图分类号: TP393.04 **文献标识码**:A

Design for lwIP-based embedded gateway for CAN/Ethernet

ZHANG Wen-ya[1,2], LI En[1,2], CAI Li[1,2], LIANG Zi-ze[1]
(1. *Institute of Automation, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *School of Graduate, Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: To realize the interconnection between the nodes of Ethernet in the control center and the nodes of the CAN bus in the industry field, an embedded system based CAN/Ethernet was designed. The TCP/IP protocol was implemented by porting the lwIP and CAN application layer protocol was proposed and realized by redefining the content of the IDENTIFIER of the CAN2.0B extension data frame. A transformation protocol was proposed and implemented to realize the data transformation between the two protocols and the control of the communication. The communication between the server of the Ethernet and the CAN nodes and the communication between the CAN nodes with different gateways were realized.

Key words: CAN bus; ethernet; gateway; lightweight TCP/IP stack (lwIP)

0 引言

CAN 总线(Controller Area Network)即控制局域网,是一种有效支持分布式控制或实时控制的串行通信网络,具有成本低、可靠性高、抗干扰性强和实时性好的特点,广泛应用于安全监控领域。随着 Internet 的发展和生产自动化程度的提高,管理人员希望能够通过 Internet 或局域网来监控工业现场的情况,这就需要 CAN 总线和 Ethernet 的互联。另外,由于 CAN 总线的最远通信距离为 10km,最大节点数为 110 个,为了增加传输距离和扩大网络容量,也需要 CAN 和 Ethernet 的互联。由于 CAN 总线和 Ethernet 采用的是不同的通信标准,要实现它们之间的互联就要通过总线标准转换设备(即网关)来实现。

本文设计了以 ARM9 为控制核心,以 Ethernet 物理层芯片和 CAN 控制收发芯片为通信接口的嵌入式网关,通过移植嵌入式实时多任务操作系统和精简的 TCP/IP 协议栈 lwIP 实现了工业以太网和 CAN 总线之间的通信协议转换。以太网的通信接口设计可以有多种方式,其中文献[2]通过移植内嵌 TCP/IP 协议栈的 μClinux 来实现 Ethernet 通信,文献[1]、[3]中用内嵌 TCP/IP 协议的控制芯片来实现与以太网的接口。和这两种接口方法相比,本文的方法具有占用资源少、实时性高、成本低、协议功能完整的特点,更加适合在监控系统中使用。

1 CAN/Ethernet 网关设计中的主要问题

一般较为庞大的监控系统采用如图 1 所示的结构方式。图中位于工业现场的 CAN 节点负责监控现场的信息并通过网关把监控信息传给控制中心的工作站和服务器,工作站则把对现场设备的设置或控制命令通过网关传给 CAN 节点;同一网关下的 CAN 节点和通过 CAN 总线实现互控和信息共享;不同网关下的 CAN 节点则要通过两个网关的转换来实现该功能。因此要实现 CAN 总线和 Ethernet 的互联,就需要实现以下四种方式的正常通信:

1)任何一个 CAN 节点都能收到工作站或服务器的数据,并可获知其来源;

2)任何一个 CAN 节点都能向工作站或服务器发送数据,并需要向服务器提供数据的来源(即本机所在网关的 IP 地址和本机 CAN 地址);

3)任何一个 CAN 节点都能和其他网关下的 CAN 节点互相发送数据,并向对方提供数据来源;

收稿日期:2006 - 08 - 09;**修订日期**:2006 - 10 - 12
基金项目:电子信息产业发展基金;北京工业大学自动化系现场总线北京市重点实验室开放资金
作者简介:张文亚(1983 -),男,河南陕县人,硕士研究生,主要研究方向:无线传感器网络、智能控制; 李恩(1979 -),男,山东滨州人,博士研究生,主要研究方向:巡线机器人、嵌入式系统; 蔡丽(1975 -),女,浙江建德人,博士研究生,主要研究方向:智能机器人; 梁自泽(1963 -),男,贵州人,副研究员,主要研究方向:智能控制、先进机器人控制、先进制造系统.

4)任何一个 CAN 节点可以和同一网关下的其他 CAN 节点进行数据交互,并向对方提供来源。

以上通信方式中,除了第四种不需要进行 CAN 总线到 Ethernet 的转换之外,其他方式都需要由网关实现协议转换。由于 Ethernet 采用的是 TCP/IP 协议,而 CAN 总线采用的是 CAN2.0 协议,而且两种协议在数据帧的结构和通信控制的各方面都不相同,要实现以上的通信过程,网关需要实现三种协议:网关和 CAN 节点通信时的 CAN 协议、和服务器通信时的 TCP/IP 协议、两种通信标准的转换协议(简称通信转换协议)。

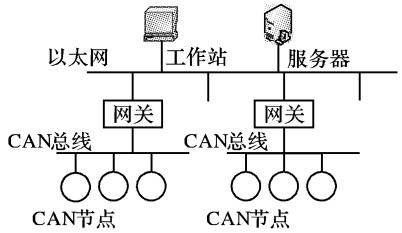

图 1　监控系统结构

2　网关的实现

系统网络的协议结构示意图如图 2,图中的第一层和第二层为通信转换协议的两层,从图中可以看出网关设计中需要实现 TCP/IP 协议接口、CAN 协议接口和通信转换协议三个部分。

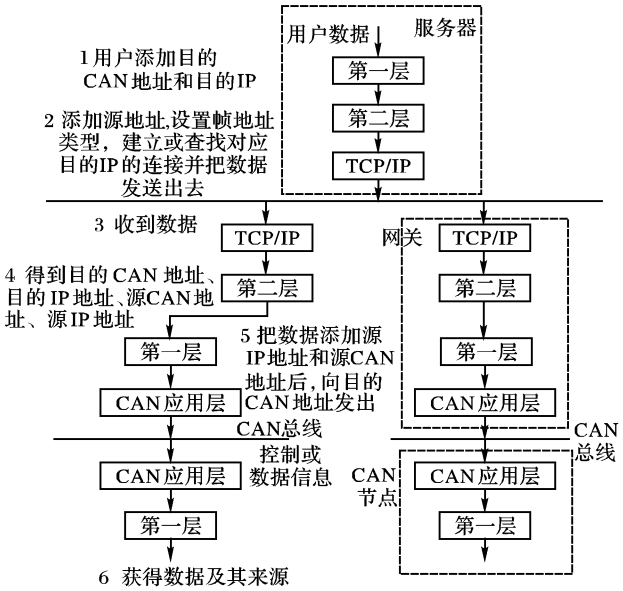

图 2　系统的协议结构和通信流程

2.1　lwIP 的移植和 TCP/IP 协议的实现

在已有的 CAN/Ethernet 嵌入式网关设计中,通常通过向 32 位处理器中移植内嵌 TCP/IP 协议的 μClinux 等操作系统,或直接采用硬件自身带有 TCP/IP 协议的处理器来实现 TCP/IP 协议栈功能,并通过 Ethernet 的控制芯片实现以太网通信。这两种方式中,前者的 μClinux 操作系统不但占用资源较多而且实时性不好,不适于实时性要求很高的实时监控系统;后者的网络处理器只是内嵌了 TCP/IP 协议的部分功能,而且由于这类处理器通常为较低档的 8 位机,当网关下的数据量很大时,就会造成较大的延迟。本文采用了开源的实时嵌入式操作系统和可裁减的 lwIP 来实现该功能,不仅保证了系统的高实时性,而且增强了网关设计的灵活性。

lwIP(Lightweight TCP/IP stack)是瑞士计算机科学院计算机和网络结构实验室的 Adma Dumkels 等开发的一套开放源码的 TCP/IP 协议栈的精简的实现,目的是在保证 TCP 协议完整的情况下减少系统资源的需求,使之适合于资源较少的嵌入式系统应用。它的最新版本包括了 IP、ICMP、TCP、UDP、DHCP、PPP 和 ARP 等常用协议的所有或部分功能,而且提供了类似于伯克利 TCP/IP 的 API 函数,完全可以满足网关的需要。

通常 TCP/IP 的实现有三种进程模型:按照 TCP/IP 协议的层次结构每层协议都用一个线程实现;在操作系统的内核中实现 TCP/IP 协议;所有的协议在一个线程中实现。lwIP 采用的是最后一种,第一种模型虽然层次结构比较清晰,系统的调试也比较容易,但是层间的交互会引起频繁且耗时的任务切换,第二种模型则依赖于特定的操作系统,重用性不好,而 lwIP 避免了以上两个问题,其缺点就是要等待系统分配资源,而这在任何系统中都是不可避免的问题。

除了实现 TCP/IP 协议的模块外,lwIP 还包括操作系统模拟层等几个支撑模块。为了使协议适用于不同的操作系统,lwIP 中所有系统函数的调用和数据结构的使用都通过系统模拟层来实现,它为系统的诸如定时器、进程同步和消息处理等服务提供了一个通用的接口,当把 lwIP 移植到某个特定的操作系统时,只要实现系统模拟层就行。lwIP 提供了诸如任务(或线程)的创建 sys_thread_new( ) 函数,任务之间的同步 sys_arch_protect( ) 和 sys_arch_unprotect( ) 函数,以及信号量和消息邮箱的产生、清除、等待和设置等和操作系统相关的接口函数,只要实现了这些函数就完成了 lwIP 在特定操作系统上的移植。

2.2　CAN 应用层协议的提出和实现

CAN 协议是建立在 ISO 的开放系统互联模型的基础上的,取其中的三层:物理层、数据链路层和应用层。物理层和数据链路层的功能可由 CAN 接口芯片来实现,而应用层的功能则要靠应用程序来完成。工业中广泛应用的应用层协议有 DeviceNet 和 CANOpen 等几种,但是这些协议都有过于复杂及成本高的特点,不适合在嵌入式系统中使用,这里采用了根据监控系统的需求而自主设计开发的应用层协议[4]。该协议通过对 CAN2.0B 帧结构的分析,对扩展帧的报文标志符的各位进行了重定义,用来存放通信中的控制信息,8 字节长度的数据场可以全部用来存放通信数据,提高了通信效率。基于管道技术设计了支持多线程通信的应用层通信协议,实现了监控系统中的命令和数据并行传输。基于帧号和位图进行数据包的拆分与重组,解决了由于 CAN 总线本身的短帧结构所造成的大数据量传输困难的问题。

应用层协议中数据的滤波和通信的控制主要通过 CAN2.0B 扩展帧的 29 位标志符来完成,其帧结构如图 3(a)所示,图中的各位从左到右依次为 ID28 到 ID0。帧头的 0 为紧急标志,通常情况下该位为 0,当 CAN 节点发送报警或服务器发送要求马上响应的控制信息时,把该位置 1,就把该帧的优先级提到了最高,能保证这些关键信息的及时发送;目的地址表明了数据的目的 CAN 节点地址,完成信息滤波;类型表明 CAN 帧的数据场中发送的是数据信息还是通信中的控制信息,由于 CAN 协议的差错控制和拥塞控制等通信控制都由硬件电路完成,所以这里的控制信息指的是应用层通信的控制;源地址表明数据的来源;帧号表明该数据的帧块序号,

当发送大块数据时,由于 CAN 每帧最多只能发送 8 个字节,所以必须把数据分块,而帧号表明了该帧数据的序号,以便于接受方对数据重组。管道号标志了虚拟通信通道的序号以及是否有空闲的通信通道,4 位的管道号表明可以同时有 16 条通信通路,可以保证多线程的实施;帧尾的 1 位是结束标志符,表明了该数据包传输的结束。

ID28	ID27–ID21	ID20	ID19–ID12	ID12–ID5	ID4–ID1	ID0
紧急标志	目的地址	类型	源地址	帧号	管道号	标志位
1bit	7bit	1bit	7bit	8bit	4bit	1bit

(a)CAN应用层帧结构

类型	CAN地址	IP 地址	数据
1bit	7bit	8bit	任意长

(b)发送数据帧结构

0x7e	类型	目的 CAN 地址	目的 IP 地址	0	源 CAN 地址	源IP地址
8bit	1bit	7bit	8bit	1bit	7bit	8bit
数据						0x7e
小于1kbyte						8bit

(c)转换协议帧结构

图 3 几种帧结构

2.3 转换协议的提出和实现

2.3.1 转换协议和通信的实现

为了实现 CAN 协议和 TCP/IP 的转换,本文提出了一个通信转换协议,包括两层,第一层定义了服务器或 CAN 节点和网关通信的数据格式,第二层为协议转换部分的数据帧格式。两层的格式分别如图 3(b)、(c)所示,其中表格下面的数字表示数据帧中对应域的长度。通信时,用户(CAN 节点或服务器)首先按照图 3(b)的格式把带有目的地址的数据传给网关,网关中的第二层协议把收到的数据编码、打包,选择相应的通信线路后向目的地址发送。下面结合图 2 分别从三条数据通路(即服务器向 CAN 节点发送数据、CAN 节点向服务器发送数据和 CAN 节点向其他网关下的 CAN 节点发送数据)来说明采用了本文的通信转换协议的 CAN 节点和以太网节点通信的流程。

服务器向 CAN 节点发送数据:

1)用户通过转换协议第一层把数据添加目的 IP 地址和目的 CAN 地址后,提交给转换协议第二层,要求第二层发送;

2)转换协议的第二层把第一层的数据加上源 IP 地址和源 CAN 节点地址(此时为 0,表示发送方为服务器),并按照第一层提供的目的 IP 地址建立或选择对应于该地址的 TCP/IP 连接,通过 Ethernet 把数据发送出去;

3)网关收到来自 Ethernet 的数据;

4)网关中转换协议的第二层收到 TCP/IP 层传来的数据后,从数据包中得到目的 CAN 地址、源 CAN 地址和源 IP 地址后,把这些地址和有效数据传给协议第一层;

5)网关中转换协议第一层把有效数据加上源 IP 地址和源 CAN 地址后,根据收到的目的 CAN 地址,通过 CAN 应用层把数据发送到目的 CAN 节点;

6) CAN 节点收到有效数据及其来源(源 IP 地址和源 CAN 地址)。

CAN 节点向服务器发送数据:

这个流程和上述服务器向 CAN 节点发送数据的流程类似,但是这时是 CAN 节点使用转换协议把数据打包后发给网关,网关把数据转换后发送到服务器,服务器则用转换协议解包得到数据和来源。

CAN 节点向其他网关下的 CAN 节点发送数据:

这时发送方的处理流程和 CAN 节点向服务器时的流程相同,但是接收方为 CAN 节点,所以接收方网关收到数据后的处理过程和服务器向 CAN 发送数据时的 3)到 6)相同。

2.3.2 转换协议的帧格式

转换协议两层的帧格式分别如图 3(b)、(c)所示。

第一层:

帧头的 1bit 的类型表明了目的 IP 地址为服务器(1)还是其他网关,用它结合目的 IP 地址的值可判断用户所加的 IP 地址是否为系统中合法的 IP 地址;

CAN 地址:因为 CAN 总线最多可带 110 个设备,所以用 7 位就可以表示,它指明了数据的目的 CAN 地址,若目的地为服务器,则该域为 0;

8 位的 IP 地址表示了数据的目的 IP 地址(服务器或网关);

由于 CAN 和 TCP/IP 都有把数据包拆分和重组的功能,所以该数据可任意长,但是为避免长数据帧的频繁重发,降低网络效率,可根据实际情况确定数据包的最大长度。

第二层:

帧头和帧尾的 0x7e 标志着一个数据帧的开始和结束,为了避免帧中其他数据和标志冲突,帧中有效数据中的 0x7e 用两个字节 0x7d 和 0x5e 表示,0x7d 用 0x7d 和 0x5d 表示。这两个标志保证了没有数据长度的情况下对数据整的完整收发;

1 位的类型表示了源 IP 地址为网关(0)还是服务器(1),它结合源 IP 地址可判断数据源是否正确;

目的 IP 地址可使网关判断收到的数据接收方是否为本机;目的 CAN 地址向网关提供了数据的目的地址;

源 IP 地址和源 CAN 地址在网关中被传给转换协议第一层,用来向用户说明数据的来源,没有来源的数据对用户来说是毫无意义的;

这里对有效数据的长度作了限制,原因就是为了避免重发过长的数据帧,降低网络的利用效率;

还有一位的预留位,通常情况下以 0 表示。

2.3.3 通信控制

上节中实现了三种条数据通信方式,为了保证通信的正常进行,还要对通信过程适当的控制,由于 CAN 协议和 TCP/IP 协议都有各自的差错控制、拥塞控制及超时重传等控制机理,所以这里只需进行连接维护,以确保服务器、网关、CAN 节点在任何一者意外重启后都可以重新建立新的连接,维持系统长时间的工作。

本文对连接的维护是基于以下两个假设完成的:

1)系统中只有两个服务器直接和 CAN 节点通信(在大多数实际系统中也是如此,一台用来监控,另一台作为热备份);

2)不同网关下的 CAN 节点之间只进行间歇性的通信。因此在网关中共有四条 TCP 连接通路,两条用于 CAN 节点和服务务器之间的通信,另外两条用于不同网关下 CAN 节点之

间的通信,它们用连接方的 IP 地址来标识。

为了保证控制中心对现场的实时监控,网关和服务器的连接不能中断,当发现连接故障时,马上进行重连。用于不同网关下 CAN 节点通信的 TCP 连接分为两类:本网关作为连接的服务器端(Server 连接)和本网关作为连接的客户端(Client 连接),前者有一个超时标志,两个连接的状态变换如图 4 状态机所示。Server 连接初始处于侦听状态,当收到对方的连接请求时,进入通信状态,开始通信;若该连接上没有数据传输,则开始记录超时并进入空闲状态,在达到超时以前若该连接又有数据传输,则超时复位,进入通信状态,否则断开该连接,进入侦听状态,等待新的连接。Client 连接初始并不存在,当网关要和其他的网关通信而没有找到对应其 IP 地址的 TCP 连接时,Client 连接进入连接状态并尝试连接目的 IP,建立连接后进入通信状态,同样根据有无通信数据,Client 连接在通信和空闲两个状态之间转化;在通信或空闲状态,若网关要和某个 IP 地址通信,但是又没有找到对应于该 IP 地址的 TCP 连接时,就断掉当前的 Client 连接,开始建立和该目的 IP 之间的连接,Client 连接不会因为空闲时间过长而断开,这样就避免了网关要连接的下一个 IP 同样是该 IP 地址时,重新连接引起的迟延。

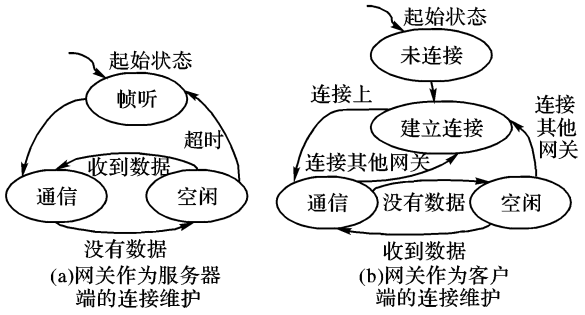

图 4　连接维护状态机

以太网中服务器端连接的建立和维护也通过转换协议第二层来完成。在服务器端,为了保证通信的实时性,服务器和每个网关都建立了连接,在发现连接故障时(比如当发送数据或接收数据多次失败时),重新建立连接。这样就保证了连接的不间断和服务器和各个网关之间通信的独立性。

3　应用实例

上述网关在煤矿安全监控系统中得到了应用。该系统共分为三层:上层为管理中心和服务器构成的光纤环网,以数据分站为节点的 CAN 总线通过网关和光纤环网的主机通信,最下层为一传感器为节点的 485 总线它直接和分站通信,完成数据采集。正常情况下分站通过网关把传感器的数据信息、报警信息和故障信息等数据通信传给服务器,服务器也通过网关向分站发送控制信息;当某一个区域发生事故时,分站就可以通过网关把事故信息和断电等控制信息发给其他网关下的分站,实现了不同区域的实时互控,避免了瓦斯事故的发生与扩大。

4　结语

本文设计了 Ethernet/CAN 嵌入式网关,基于嵌入式 lwIP 协议栈的移植实现了 TCP/IP 协议,通过重新定义扩展帧报文符的结构实现了 CAN 应用层协议,根据地址转换所提出的转换协议实现了协议的转换和网络连接的维护。在煤矿安全监控系统中的应用证明了该网关的可靠性。

参考文献:

[1] 曹洋. 以太网与 CAN 总线间网关的设计与实现[J]. 微型机与应用,2004, 23(9):28 - 30.

[2] 杨波,徐成. 嵌入式 CAN-Ethernet 网关的设计与实现[J]. 计算机应用,2005,25(2):273 - 275.

[3] 梁泰文,阳宪惠. CAN/Internet 嵌入式网关的一种设计方案及实现[J]. 冶金自动化,2004,28(2):5 - 10.

[4] 李恩,蔡丽,梁自泽,等. 一种适用于煤矿安全监控系统的 CAN 总线应用层通讯协议[J]. 计算机应用,2006, 26(9): 2178 - 2181.

[5] STEVENS WR. TCP/IP 详解第一卷: 协议[M]. 北京: 机械工业出版社, 2002.

[6] ABROSSE JJ. μC/OS-II——源码公开的实时嵌入式操作系统[M]. 北京: 中国电力出版社, 2001.

[7] GMBH RB. CAN Specification version 2.0[Z]. 1991.

[8] DUNKELS A. Design and Implementation of the lwIP TCP/IP Stack [Z]. Swedish Institute of Computer Science. 2001.

(上接第 277 页)

示,随着网络负载的增加,IEEE802.11DCF 的数据丢包率远远高于 APSM,这主要因为 APSM 减少了数据流对共享无线信道的竞争和转发节点大量积聚数据包的丢弃。更广泛的仿真表明,APSM 的拥塞反馈机制减少了控制报文的数量,APSM 的退避算法提高了信道接入公平性。

4　结语

IEEE802.11DCF 在无线自组网中性能较低,二进制指数退避算法不能根据网络的实际竞争状况进行调整,公平性差,时延抖动大,MAC 层竞争机制会导致业务流局部拥塞,影响业务流性能。本文基于 IEEE802.11DCF 提出 APSM 来解决上述问题。它主要包括网络适应性退避算法和拥塞反馈两个机制。网络适应性退避算法的主要思想是引入网络竞争状况因子调整节点退避计数器的取值,其特点是使退避计数器值的变化和节点附近的真实竞争状况紧密联系,保证接入的有效性、公平性,并避免退避计数器值剧烈变化。拥塞反馈机制的主要思想是将局部拥塞信息反馈给上游节点,使上游节点降低发送速率或停止发送数据包。仿真结果表明,APSM 有效地提高了网络性能,较大地降低了数据丢包率,较好地解决了接入公平性问题,降低了端到端平均时延。

参考文献:

[1] ISO/IEC 8802 - 11: 1999(E), IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications[S].

[2] XU S, SAfADAWI T. Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc networks[A]. IEEE Communications Magazine[C]. 2001. 130 - 137.

[3] KOKSAL CE, KASSAB H, BALAKRISHNAN H. An Analysis of Short-Term Fairness in Wireless Media Access Protocols[A]. ACM SIGMETRICS 2000[C]. Santa Clara, CA, June 2000.

[4] TALUCCI F, GERLA M, FRATTA L. MACA-BI(MACA by invitation)-A Receiver Oriented Access Protocol for Wireless Multihop Networks[A]. Proc. IEEE PIMRC'97[C]. Sept 1997.

[5] YI Y, SHAKKOTTAI S. Hop-by-hop congestion control over a wireless multi-hop network[A]. Proc. IEEE INFOCOM[C]. 2004.