

基于3G网络远程访问和监控系统的设计与实现

张 军, 李长云, 崔海燕, 田得润, 戴明华

(湖南工业大学 计算机与通信学院, 湖南 株洲 412008)

摘 要: 在 Windows CE 嵌入式平台上设计与实现了基于 3G 网络的远程访问和监控系统。介绍了系统架构, 阐述了在 3G 网络移动设备上设计远程访问终端的技术, 基于 SOCKET 技术定义了统一的监控数据交换协议。该系统实现了实时多点监控和远程移动访问, 并通过实践验证了系统的有效性。

关键词: 远程访问; Windows CE; 嵌入式平台; 3G 网络

中图分类号: TP277.2

文献标志码: A

文章编号: 1673-9833(2011)06-0100-05

Design and Implementation of 3G-Based Remote Access and Monitoring System

Zhang Jun, Li Changyun, Cui Haiyan, Tian Derun, Dai Minghua

(School of Computer and Communication, Hunan University of Technology, Zhuzhou Hunan 412008, China)

Abstract: Designed and implemented a 3G-based remote access and monitoring system on the Windows CE embedded platform. Introduced the system architecture, described the technology to design remote access terminals on 3G mobile device, and defined the unified monitoring data exchange protocol based on SOCKET technology. The system realized a real-time multi-point monitoring and remote mobile access, and verified the validity of the system through practice.

Keywords: remote access; Windows CE; embedded platform; 3G wireless network

0 引言

远程监控是一种监控端与被监控对象在物理位置上分开, 通过网络来获得信息和对远程计算机进行操作的系统。在国内外, 远程监控的应用十分广泛。目前, 大部分的监控系统都是以计算机为核心, 多媒体技术、网络通信技术、传感器技术及自动控制技术相结合来构建的^[1]。

嵌入式技术及移动通信技术的蓬勃发展给远程监控技术带来了革新, 为现代社会的生产生活实施

数字化的网络监控提供了有力的技术保障。近年来, 国内外对基于无线移动通信的远程监控技术研究火热, 且该项技术已经广泛应用于无线抄表、变电站监控、航标灯控制、水文气象监控、远程遥控等智能控制领域中^[2]。3G 牌照发放后, 国内电信运营商积极进行 3G 网络建设, 高速数据传输技术的发展为工程应用提供了有力支持。但基于 3G 网络的无线远程监控, 目前还存在诸如开放性、可靠性较差及应用开发较难等问题。基于上述背景, 本文提出了一种基于 3G 网络的远程访问和监控系统, 定义了一种开

收稿日期: 2011-09-05

基金项目: 国家技术创新基金资助项目(11C26214302856), 中国博士后科学基金资助项目(20080440216), 湖南省自然科学基金资助项目(11JJ4050), 湖南省教育厅科学研究基金资助项目(09C326)

作者简介: 张 军(1984-), 男, 河南信阳人, 湖南工业大学硕士生, 主要研究方向为嵌入式应用和可信软件,

E-mail: zhangjun6_26@163.com

通信作者: 李长云(1972-), 男, 湖南耒阳人, 湖南工业大学教授, 博士后, 主要从事可信软件和软件动态演化方面的研究,

E-mail: lcy469@163.com

放的系统框架,其具有适应性强、传输速率高等特点,还可支持手持式智能设备的远程访问。

1 系统架构

基于3G网络的远程访问和监控系统由监控前端、监控中心、移动访问查询端3个部分组成。该系统构成如图1所示。

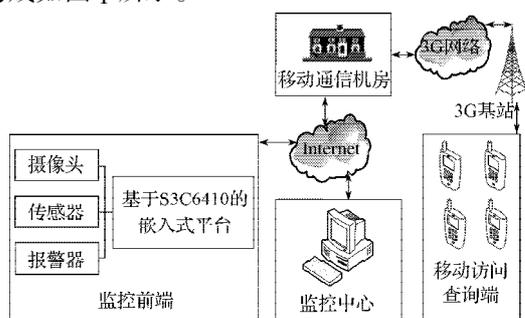


图1 系统组成图

Fig. 1 The system diagram

1) 监控前端。其部署在监控现场,主要功能是对前端采集及报警设备进行控制管理,从监控现场采集信息,对采集的数据进行压缩、打包及转发,解析和执行由监控中心发送的控制指令并及时将反馈信息和现场各设备的状态信息发回监控中心。在前端部署一个嵌入式平台,该平台提供了接口与前端的具体采集设备相连,本文采用处理能力强、稳定性好的S3C6410处理器芯片作为该平台的核心。

2) 监控中心。这是整个系统的核心,其主要功能是数据存储发送控制指令。工作流程是:初始化、启动网络服务和等待远程监控前端的连接请求;维护监控前端及用户列表,验证用户登陆;用户登录后,可随时向监控前端发送控制及监测指令;移动访问查询端可随时向监控中心发送连接请求,连接后,可实时查询和调取监控数据或监测监控现场;对数据进行存储、检索、回放等。

3) 移动访问查询端。它为3G移动智能设备(如3G智能手机、PDA等),主要功能是远程访问。该端先连入网络,动态获取一个IP地址,再向监控中心发送连接请求,验证登录后,用户可随时随地地查询感兴趣的监控信息,也可发送一些基本的控制指令,经监控中心审核与处理,再由监控中心转发至监控现场。

2 关键技术及系统的具体实现

2.1 监控前端的设计和实现

将经裁剪与优化的Windows CE6.0嵌入式操作系统和经编译的应用程序一起移植到S3C6410芯片的

Nand Flash中。嵌入式数据库SQL Server CE3.0存储前端所有设备及自身的状态信息和部分监测数据。前端还可智能控制报警器报警,增强了系统的安全性、可靠性。监控前端结构框架如图2所示。

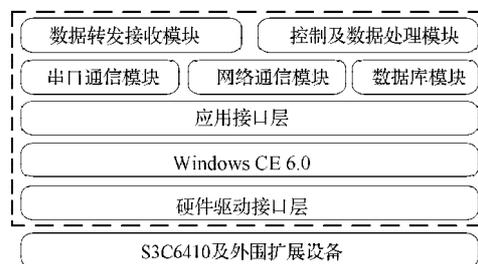


图2 监控前端系统结构图

Fig. 2 The structure diagram of front-end monitoring system

2.1.1 嵌入式操作系统及数据库的设计和实现

Windows CE6.0是一款高度模块化的嵌入式操作系统,具有可裁剪性与稳健的实时性,支持多硬件平台以及与之配套的开发工具^[3]。具体实现过程如下:

1) 基于BSP源代码^[4]开发BSP(即板级支持包)。首先,建立引导程序(BootLoader),其功能是将Windows CE操作系统加载到内存,为系统初始化各种参数,按结构可分为BLCommon、OEM、EBoot、存储管理、EDBG驱动程序5个部分,除了OEM代码自己编写外,其它都是由Windows CE自身提供,OEM的功能是控制和调试硬件平台。其次,开发OAL和驱动程序,OAL是把操作系统内核对硬件的访问功能抽象出来,形成一些函数或者库,实现内核和目标硬件之间的通信,包括处理中断、计时器、电源管理、通用I/O控制等。驱动程序直接与硬件外设打交道,是应用程序或操作系统与硬件外设交互的桥梁。在Windows CE下,该程序以用户态下的DLL文件形式存在,编写该程序所用到的方法、工具与编写其它普通的DLL相同。

2) 裁剪定制操作系统。启动BSP后,通过开发工具Platform Builder创建一个新的平台。根据系统需求,添加内核组件,加入网络和串口支持、Direct Show相关的及运行必要的组件服务,对字体的选择要慎重,一般不要添加太多字体,这样能保证最小的运行内核;裁剪Windows CE内核不需要的组件,不添加微软直接发布给用户的应用程序,这样能避免Platform Builder自动搜索该程序的相关组件并加入系统中,造成系统体积过大,不能很好地保证系统的最小运行。

3) 嵌入式数据库SQL Server CE具备精简的数据库引擎和强大的查询优化器,提供了与SQL Server一致的开发模型和API,支持远程数据访问和

合并复制, 离线修改数据后能与服务器同步, 且占用很少的内存和系统资源, 因此是嵌入式无线环境的理想选择。数据库模块的功能包括前端数据采集和报警设备基本信息管理 2 个部分。数据表包括设备状态表、设备配置表及采集数据表。SQL CE 数据同步常用的方式有远程数据访问和合并复制, 本系统采用远程数据访问。OLE DB 技术可方便地访问 SQL CE, 是微软开发的一种基于 COM 的高性能数据库技术, 提供了一种统一的数据访问方式, 用户可通过该接口访问数据, 把数据库组织成一个合作组件基地。OLE DB 的主要接口有: IDBInitialize, 用于初始化和释放数据源对象; IDBDataSourceAdmin, 用于新建数据库; IDBCreateSession, 用于获取一个新的数据库访问会话对象; IDBCreateCommand, 用于创建一个新命令对象; ICommandText, 用于表示文本命令对象; ITransactionLocal, 用于执行事务。

2.1.2 串口及网络通信模块的实现

串口是与前端具体采集设备及报警器进行通信的数据接口, 具有连接线少、通讯简单等特点^[5]。根据距离的远近来选择接口方式, 长距离用 RS485, 短距离用 RS232。具体实现如下:

1) 通过 CreateFile 函数打开 COM1 端口。

```
HANDLE hComm = CreateFile( _T( " COM1: " ),
    GENERIC_READ|GENERIC_WRITE, 0, NULL,
    OPEN_EXISTING, 0, NULL);
```

2) 设置串口参数 (波特率、奇偶校验、数据位等)。先调用 GetCommState 函数获取串口的当前状态信息, 再调用 SetCommState 函数配置串口, 调用 GetCommTimeouts 和 SetCommTimeouts 函数对串口读写操作的超时参数进行设置。

3) 调用函数 ReadFile 和 WriteFile 对串口进行读写操作。由于 Windows CE 不支持重叠 I/O 操作, 为了防止串口的读写阻塞主线程中处理主窗体的消息队列, 可采用多线程技术来处理, 即分别用单独的线程去读写串口, 通过多线程来模拟重叠操作。

网络通信模块是为监控中心与前端和查询端之间提供安全可靠的数据传输链路。Windows CE 支持 TCP/IP 协议, 而 Socket 是一种底层的通信机制, 通信双方必须根据约定的协议对数据进行处理和解释, 因此本文采用支持流连接和数据报连接的 Socket 模式。在流连接中, 套接字是一个基本数据管道, 当两点连接时, 数据会来回传送, 不需要额外附加地址; 在数据报中, 套接字像邮槽, 离散数据包会附加目的地址^[6]。本文根据传输数据类型的不同来自动选择数据传输方式。因 Windows CE 不支持异步套

接字, 所以采用多线程技术。

2.1.3 数据接收转发和数据管理控制模块的实现

数据接收转发的主要功能是: 从监控中心获取控制指令和控制参数, 经处理后直接发向监控前端; 接收监控前端反馈的状态信息和采集的现场数据, 经处理传向监控中心, 同时将设备状态信息写入嵌入式数据库, 作为系统运行日志。数据处理主要是对传输数据按照协议要求进行打包封装, 对某些数据 (如关键的系统配置信息和验证信息等) 进行加密, 对接收数据进行拆包, 对控制指令进行解析等。受嵌入式芯片容量限制, 该模块不能存储大量的数据, 因此该模块和监控中心的数据库之间要遵循一定的协议来清理存储空间。系统实现了自动报警功能, 若前端采集的某些数据及状态信息满足报警规则, 就发出报警信号。

2.2 移动访问查询端的设计

该端运行平台是以 Windows Mobile6 为操作系统的 3G 手机或 PDA。为了保证系统的安全性, 防止未经授权的手机设备连入监控中心, 需先通过 Windows Mobile6 提供的 GetDeviceUniqueID 函数来获取智能设备的唯一标识即注册编码, 在监控中心注册, 再从注册表中读取监控中心的 IP 地址和端口号 (首次启动需配置该 IP 和端口号), 然后向监控中心发送连接请求, 通过监控中心的验证后, 建立连接, 并创建一个接收线程, 接收由监控中心发送的数据包, 交由主线程解析处理。部分代码如下:

```
…… // 通过监控中心的验证, 建立 TCP 连接
RECVPARAM *pRecvParam=new RECVPARAM;
// 自定义结构体为新建线程参数
pRecvParam->sock=m_mainSocket;
pRecvParam->hwnd=m_hWnd;
HANDLE hRecvThread=CreateThread(NULL,0,
RecvProc,(LPVOID)pRecvParam,0,NULL); //创建接收线程

CloseHandle(hRecvThread);
……// 控制及查看指令的发送
DWORD WINAPI Z_MobileClientDlg::RecvProc(
    LPVOID lpParameter )
{
    SOCKET sock=((RECVPARAM*)lpParameter)->sock;
    HWND hwnd=((RECVPARAM*)lpParameter)->
hwnd;
    delete lpParameter;
    while(TRUE)
    {
        char *recvbuff=new char[PACKET_SIZE];
```

```

int result=recv(sock,recvbuff,PACKET_SIZE,0);
.....
// 向主窗体发送消息, 请求对数据包的解析处理
::PostMessage( hwnd,WM_DATAPROCESS,
(WPARAM)result,(LPARAM)recvbuff);
}
}
LRESULT Z_MobileClientDlg::OnDataProcess(
WPARAM wParam,LPARAM lParam)
{
..... // 数据包解析及数据处理
}

```

2.3 监控中心的设计

监控中心是整个系统的核心, 负责数据存储及与监控前端的嵌入式平台通信, 还负责移动访问查询端的随时访问查询。主要由7个模块组成:

- 1) 网络连接监测模块。负责监视监控中心的网络连接情况及网络负荷, 当检测到网络断开时, 立即报警, 重新连接网络, 以保障数据的传送。
- 2) 网络通信模块。采用Socket技术, 负责监控中心与前端和查询端的数据交互。主要完成Socket接口的绑定及监听、数据的接收、命令的发送等功能。

3) 数据转换模块。主要负责数据发送前对数据按照规定的协议格式进行打包封装, 对接收到的数据进行拆包解析。

4) 控制管理模块。主要负责对监控前端的控制管理, 如设置前端报警器的报警规则、前端数据库与监控中心数据库的数据同步规则等。

5) 数据存储模块。主要负责按照用户的需求, 通过网络接收监控现场的数据并按监控现场编号和时间规则存储到数据库。

6) 数据显示模块。主要负责实时数据显示、历史数据查询等。

7) 信息管理模块。对用户信息、移动端的注册信息、监控现场的基本信息等进行管理。

以上简要介绍了监控中心各个模块的功能, 具体设计与实现就不详述。

该系统采用了Client/Server的结构来实现, 将监控前端和移动访问查询端作为监控中心(Server)的2种不同类型的远程客户端(Client), 服务器与客户端通过Socket进行网络通信。为了提高系统响应速度, 多处使用子线程, 异步处理各种不同事件, 这样可避免事件之间的盲等^[7]。基于3G网络的远程访问和监控系统总体结构如图3所示。

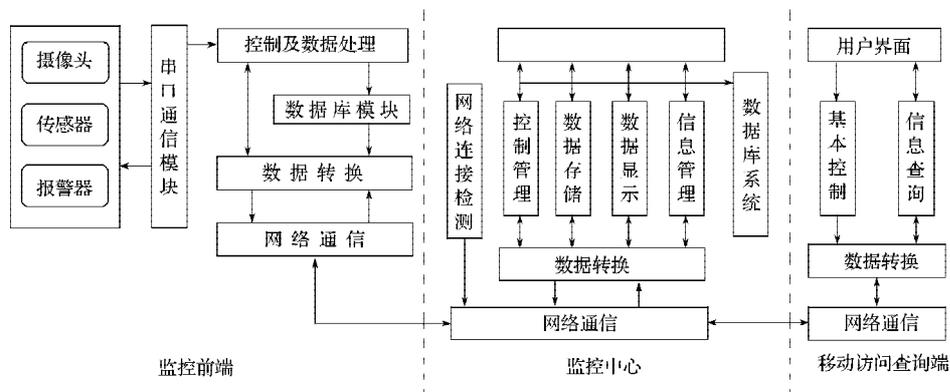
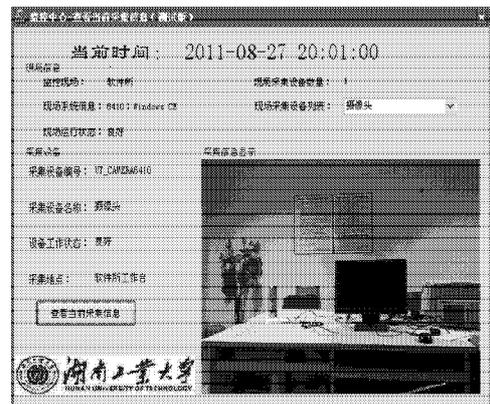


图3 系统总体结构图

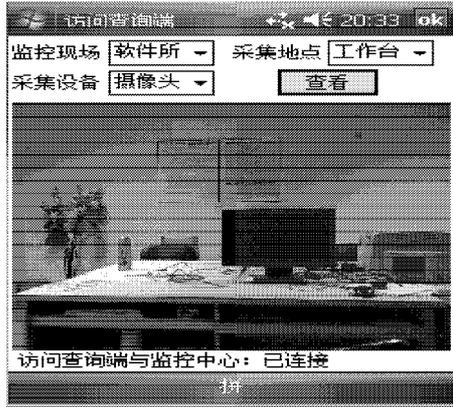
Fig. 3 The system structure chart

3 实验结果

3G网络是中国电信CDMA2000 EVDO, 移动访问查询端是HP iPAQ掌上电脑, 监控中心为Windows XP平台。先将监控前端各软件模块与经裁剪的Windows CE操作系统一块烧写到基于S3C6410的开发板中, 再将摄像头和相关监控设备连接到开发板, 系统启动后, 为监控前端和移动访问查询端配置监控中心IP地址, 同时建立连接。经测试, 移动访问查询端与监控中心的连接时间小于2s, 访问监控中心的数据响应时间小于3s, 监控前端对移动访问查询端的命令响应时间小于5s。系统运行效果如图4所示。



a) 监控中心监控图



b) 移动访问查询端监控图

图4 实验效果图

Fig. 4 Experimental effect chart

4 结语

本文基于 Windows CE6.0 嵌入式平台,设计了一种开放的远程监控系统框架,实现了多个设备的网络管理和多点监控,还支持手持式智能设备的远程访问,利用该框架能快捷地开发出适合各种应用领域的监控系统。且用 VC 开发了一个测试系统,实验证实了该框架的有效性。

参考文献:

- [1] 刘小虎,黄以平.基于嵌入式系统的串行设备远程监控系统[J].计算机系统应用,2010,19(11):43-47.
Liu Xiaohu, Huang Yiping. Serial Device Based on Embedded System Remote Monitoring System[J]. Computer Systems & Applications, 2010, 19(11): 43-47.
- [2] 刘连波.基于移动通信的通用远程监控协议的设计[D].大

连:大连理工大学,2008:2.

Liu Lianbo. Design of Mobile Communication-Based General Remote Monitoring Protocol[D]. Dalian: Dalian University of Technology, 2008: 2.

- [3] Yao Paul. 移动化时代:探索 Windows Embedded CE 6.0 的新功能[EB/OL]. [2011-06-18]. <http://msdn.microsoft.com/zh-cn/magazine/cc163502.aspx>.

Yao Paul. Mobile age: Exploration of New Function of Windows Embedded CE 6.0[EB/OL]. [2011-06-18]. <http://msdn.microsoft.com/zh-cn/magazine/cc163502.aspx>.

- [4] 辛雁峰,夏海宝,易春海.基于 S3C2440 移动终端的 Windows CE 开发[J].微计算机信息,2009,25(8):71-73.

Xin Yanfeng, Xia Haibao, Yi Chunhai. Mobil Terminal Windows CE Exploiting Based on S3C2440[J]. Microcomputer Information, 2009, 25(8): 71-73.

- [5] 李劲松.基于嵌入式Linux-ARM远程无线监控系统设计[D].北京:北京邮电大学,2009:16.

Li Jingsong. Design of Embedded Linux-ARM Based Remote Wireless Monitoring System[D]. Beijing: Beijing University of Posts and Telecommunications, 2009: 16.

- [6] Boling Douglas. Programming Windows Embedded CE 6.0 Developer Reference[M]. 4th. [S. l.]: Microsoft Press. 2007: 391-392.

- [7] 耿东久,索岳,陈渝,等.基于 Android 手机的远程访问和控制系统[J].计算机应用,2011,31(2):559-561.
Geng Dongjiu, Suo Yue, Chen Yu, et al. Design and Implementation of Android Phone Based Access and Control in Smart Space[J]. Journal of Computer Applications, 2011, 31(2): 559-561.

(责任编辑:邓彬)