一种基于PDA + GPRS的仿ISO8583通信应用方案

徐 涛， 柯文辉， 陈祖宁
(华南理工大学 软件学院,广东 广州 510656)

摘 要:针对某商业项目中需要使用PDA进行远程数据传输以及大范围现场数据采集的需求,通过对ISO8583通信协议进行改进,设计并实现了一种基于PDA + GPRS的仿ISO8583通信方案。它为金融服务业、保险业、警务行业等对通信性能有着较高要求的系统设计及开发提供了一种安全、高效的参考解决方案。

关键词: 移动数据采集;掌上计算机;通用无线分组业务
中图分类号:TP 393.04 **文献标识码**: A **文章编号**:1671 - 7147(2010)03 - 0284 - 05

Design of an ISO8583-Like Data Transmission System Based on PDA + GPRS

XU Tao, KE Wen-hui, CHEN Zu-ning
(School of Software Engineering, South China University of Technology, Guangdong 510656, China)

Abstract: To solve the communication problem of a commercial project which includes a module of data transmission system, we have designed and implemented a solution based on protocol ISO8583 and PDA + GPRS. The solution is highly efficient and reliable. It provides an efficient and secure reference for the design and development of electronic management system for industries such as financial service industry, insurance industry and police industry which needs mobile data collection.

Key words: mobile data collection, PDA, GPRS

掌上计算机(Personal Digital Assistant,PDA)相对于传统的微型计算机,具有轻便、小巧、可移动性强,同时又不失强大功能等优点。随着计算机软硬件技术的发展,PDA的CPU速度飞速提高,PDA上的操作系统日趋完善,其功能日益强大。尤其当它与现代通信技术有效地结合后,出现了可以直接接入无线局域网(WLAN)或可以直接接入GSM、CDMA等移动网络的PDA[1]。在现有的应用领域中,PDA可外扩很多配件,如RFID读写头、条码扫描头、数据采集卡,摄像头等,这些都使PDA成为具有某种特殊功能的便携终端[2]。

目前,在零售、保险、金融、证券、警务、航空、医疗等移动性和数据更新性较强的行业,PDA应用较为广泛。PDA在金融,警务,保险等行业的应用时,由于行业的特殊性,因此对其安全性及通信效率有着较高的要求[3]。作者为一家金融业服务公司开发信息管理系统,使用PDA实现服务现场远程数据的下载,采集及上传。

1 系统的分析与设计

ATM清机服务:是指包括ATM加钞、清机轧账、维修、保养、更换耗材、取吞卡、清洁等服务。

收稿日期:2010 - 01 - 04; **修订日期**:2010 - 03 - 12。
作者简介:徐 涛(1981—),男,湖北枣阳人,软件工程师。主要从事中间件与企业应用集成技术的研究。
Email:xtao@grgbanking.com

目前,随着银行服务外包业务不断发展,ATM 清机服务已逐步成为金融服务中的重要组成部分,尤其对于离行式 ATM(远离其银行网点的 ATM),因地理位置分布广,管理复杂,维护成本高,越来越多的银行将其外包给专业公司进行管理,而将主要精力放在银行的核心业务(贷款,存款)上。为了实现规范化 ATM 清机服务的作业流程,减少人工或手工工作量,提供安全的管理分配任务模式及对任务执行实现全程监控,设计开发了该清机业务管理系统。

1.1　业务流程简介

ATM 清机业务流程包括:计划员制订清机计划,安排各类资源(清机员,清机车辆,ATM 钥匙,ATM 密码信封,ATM 耗材等);清机员通过 PDA 获取任务及任务中 ATM 的详细信息(如 ATM 地址,注意事项等),领取物品,乘指定车辆按规定线路执行清机任务(如任务类型含加钞,到指定金库领取钞箱等);在清机过程中,清机员需将清机中的业务数据(如钞箱条码扫描,吞卡张数,钞箱剩余钞票张数等)通过PDA实时传回到系统中。任务执行完毕,清机员返回,上缴各类资源。PDA 通信系统模块的主要功能有:权限验证,任务下发,钞箱登记,清机记录,清机故障处理记录,状态监控。

1.2　PDA 通信模块整体设计

在此系统中,为实现对执行中的清机业务数据进行即时查询与更新,需要采集数据。考虑到 ATM 的位置分布较广,决定采用 PDA + GPRS 的方式。此系统中的 PDA 添加了条码扫描模块,用于扫描钞箱、ATM 设备、车辆、金库等上的条码,以进行数据采集。

GPRS 简介:通用无线分组业务(General Packet Radio Service,GPRS)作为第二代移动通信技术 GSM 向第三代移动通信(3G)的过渡技术,是一种基于GSM 的移动分组数据业务,面向用户提供移动分组的IP 或者 X.25 连接,可以理解为 GSM 的一个更高层次。GPRS 是利用“分组交换”(Packet-Switched)实现无线数据传输,好处是只有在有资料需要传送时才会占用频宽,而且能够以传输的资料量计价,这对用户而言是比较合理的,尤其对于需要传送较大数据量的用户是较好的选择[4]。

PDA + GPRS 在系统中的应用如图 1 所示。

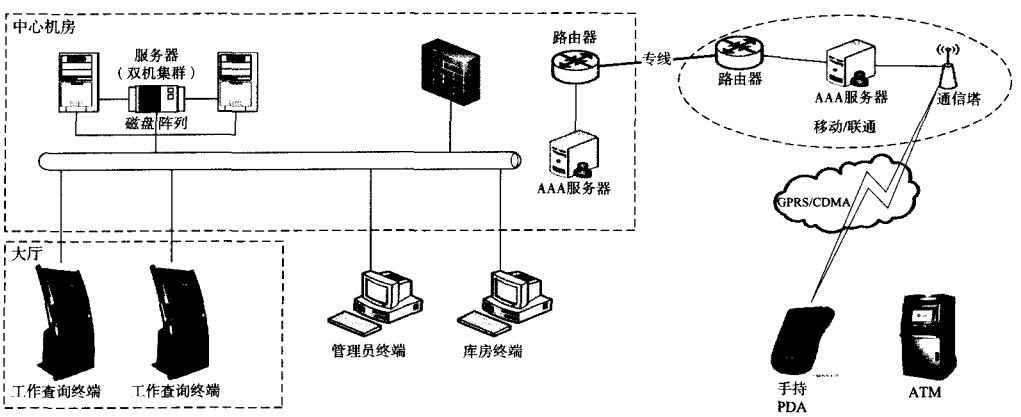

图 1　网络结构图

Fig. 1　Diagram of network structure

系统分内网和外网两部分,内网由图 1 左上角方框内的中心机房系统服务器、路由器、防火墙、网关服务器(暂时称为“AAA”)等组成,外网则由除此之外的广域网,PDA 等组成。其中“AAA”服务器负责拨号上网、各种服务代理、网络监控等功能。在路由器上设定外网与“AAA”服务器某一端口通信的所有报文均直接转发至系统服务器,从而实现 PDA 与系统服务器的网络通信。

1.3　PDA 通信模块详细设计

考虑到此系统为金融服务相关的系统,对安全性及可靠性有较高的要求,决定采用基于 C/S 架构的报文通信方式。

1.3.1　Server 端整体架构　Server 端采用 Java 开发,开发工具为 MyEclipse, Server 端整体架构如图 2 所示。

系统在启动时即建立 3 个线程,分别为主程序、报文读取线程、报文解析及发送线程。系统将接收到的报文放入待处理报文链表中,等待报文解析线程进行解析。报文解析线程不仅用以解析报文而且可以进行解析报文后的业务处理,如业务判断及操作数据库等。业务处理完成后,由报文解析线程生成相应的响应报文发给 PDA。

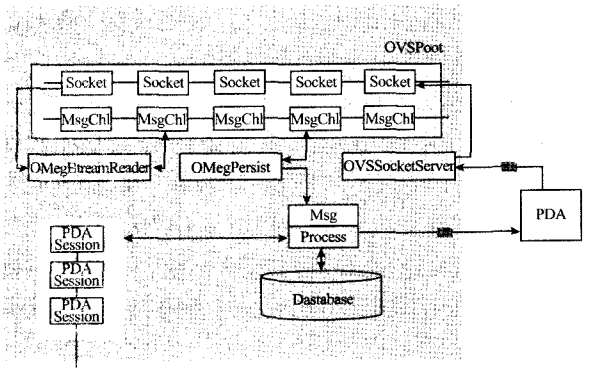

图2 Server 端程序整体架构

Fig. 2 Diagram of server structure

1.3.2 报文设计 系统初期设计时报文采用固定格式,即报文的域个数、各个域长度、总长度均为固定,其结构如图3所示。

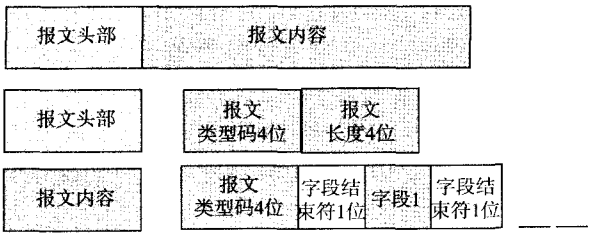

图3 报文结构

Fig. 3 Diagram of data frame

报文分为报文头部和报文内容体,报头由报文类型编号4位字符和报文体长度4位字符组成,报文内容体由报文类型编号4位字符和域结束符1个空格以及多个域和字结束符组成。

图4为报文0001登陆报文结构框架。

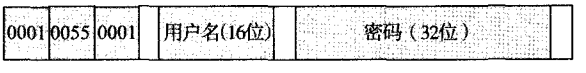

图4 登录报文结构

Fig. 4 Diagram of login data frame

此种固定格式报文的优点是结构简单,解析及构建均比较方便;缺点是扩充性差,不便于修改,如要增加或删除域均需修改源代码;另外此种设计的通信效率较低,如一个域内容为"ATM 备注",其长度设计为最大1 000字节,则在构建报文时必须填满1 000字节,否则接收端在解析时会出错。

为提高通信模块的扩充性、通用性,参考金融业常用的ISO8583包的实现方式,文中设计了一种基于8583的改进通信方式。

ISO8583包(简称8583包)是一个金融业国际标准的包格式,最多由128个字段域组成,每个域都有统一的规定,并有定长与变长之分。8583包前面一段为位图,用以确定包的字段域组成情况[5]。位图是8583包的灵魂,它是打包解包确定字段域的关键,而了解每个字段域的属性则是填写数据的基础[6]。

1) 位图描述如下:

位图位置:1;

格式:定长;

类型:B16(二进制16位,16 * 8 = 128 bit);

描述:① 如将位图的第一位设为1',表示使用扩展位图(128个域),否则表示只使用基本位图(64个域);② 如使用某数据域,应在位图中将相应的位设为1',如使用41域,需将位图的41位设为1'。

选用条件:如使用65到128域,需设位图域第一位为1'。

2) 其他域:

位图位置:每个域均有其规定的固定位置,如交易主账号信息的位图位置固定为2,此位置也决定了其在报文中的域的位置为第2域;

格式:定长或不定长,由报文定义的XML文件中域格式决定;

类型:也由报文定义的XML文件中域格式决定;

每个域的定义(C语言描述)如下:

```
typedef struct ISO8583
{
int bit_flag; /* 域数据类型 0-string, 1-int, 2-binary */
char *data_name; /* 域名 */
int length; /* 数据域长度 */
int length_in_byte;/* 实际长度(如果是变长) */
int variable_flag; /* 是否变长标志 0:否 2:2位变长, 3:3位变长 */
int datatyp; /*0-string, 1-int, 2-binary */
char *data; /* 存放具体值 */
int attribute; /* 保留 */
} ISO8583;
```

之所以参考8583,就是因为83包的解析与构建目前已经有较多的开源代码(如JPOS)可供参考。

参考JPOS对8583的处理方式,在XML中定义报文结构如下:

```
< isopackager type ="0001" name ="Login Message" >
< isofield
id ="0"
length ="4"
name ="MESSAGE TYPE INDICATOR"
```

class = "org. jpos. iso. IFA_NUMERIC"/ > 此处 class 中的 IFA_NUMERIC 表示 ASCII 码数字类型

< isofield

id = "1"

length = "16"

name = "BIT MAP"

class = "org. jpos. iso. IFB_BITMAP"/ > 此处 class 中的 IFB_BITMAP 表示 BINARY 位图

< isofield

id = "2"

length = "16"

name = "Login Name"

class = "org. jpos. iso. IFA_LLCHAR"/ > 此处 class 中的 IFA_LLCHAR 表示 ASCII 码变长字符,其长度由前两位决定

……

为了避免系统频繁读取 XML 报文配置文件,在系统启动时,即将报文配置 XML 文件读入内存中,在解析报文及生成响应报文时只需读取内存中的相应信息即可。

JPOS 中报文解析关键类简述:①ISOBitMap 封装了 protected BitSet value,并提供维护该 Bitmap 的方法;②ISOMsg 包括 fields、header、direction,消息类型是在第 0 号位存放的;③ISOChannel 用以完成底层的 package 和 interchange,是应用层与底层细节的一个联系纽带。这个类负责完成报文的发送和接收,接收的参数包括:ISOPackager、ServerSocket、host 和 port。图 5 显示了 JPOS 整体结构中的各个关键类之间的关系。

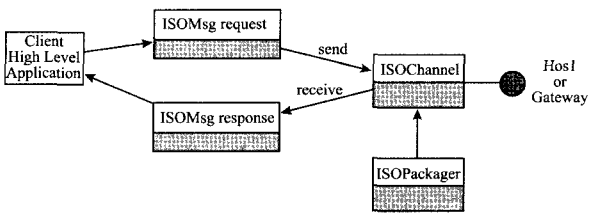

图 5　JPOS 整体结构

Fig. 5　Diagram of JPOS structure

1.3.3　Client 端设计　Client 端采用 J2ME 技术开发,开发工具为 MyEclipse。Client 端的报文解析及构建方法同 Server 端,同时采用小型数据库 RMS 实现本地数据的保存。PDA 端界面如图 6 所示。

2　系统安全

系统主要由以下 4 种措施确保安全,即每次报文均需进行用户 \ 密码验证,所有通信数据采用 Triple DES 加密算法加密,报文结构由配置文件决定。

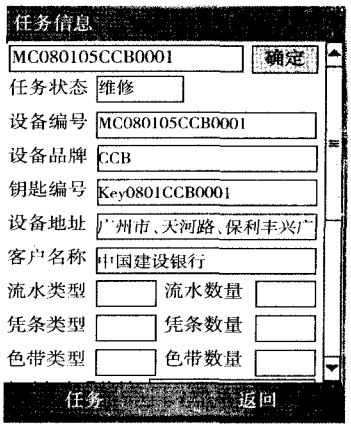

图 6　PDA 上的 Client 端界面

Fig. 6　User interface on PDA client

1) 系统在每个报文中都含有登录用户、登录密码,以验证 PDA 用户的合法性,其中密码是以 MD5 加密算法加密过的密文。系统会验证每个报文中的 PDA 用户名与密码,如验证不通过则返回登录失败报文,如验证失败次数连续超过 5 次则将锁定此用户;如用户名与密码验证通过则会进行相应的业务处理。这样当系统侵入者未获得合法的用户名及密码时,将无法窃听系统数据。MD5 加密算法:把任意长度的信息通过加密产生 128 位信息摘要(或信息指纹),这种加密算法对不同的信息不可能产生同一信息摘要,同时对于给定的信息摘要推断出其相应的信息也不可能[7]。MD5 属于单向加密的加密算法,使用 MD5 对密码加密后,加强了系统安全性。

2) PDA 与系统的所有通信数据均采用 Triple DES 加密,密钥分别保存在 PDA 的配置文件及系统的数据库中。此密钥每隔一段时间(如一个月)将更换一次。这样当系统侵入者仅得知登录用户名及密码时,如果无对应 PDA 的密钥,也无法对监听到的数据进行解密,从而无法窃取系统数据。Triple DES 是 DES 向 AES 过渡的加密算法,它使用 3 条 64 位的密钥对数据进行 3 次加密,是 DES 的一个更安全的变形。Triple DES 加密算法以 DES 为基本模块,通过组合分组方法设计出分组加密算法,比起最初的 DES,3DES 更为安全[8]。

3) 通信报文采用类 8583 报文,其结构由报文配置文件决定。即使系统侵入者监听到报文,如果没有报文配置文件,也无法对监听到的数据进行解析。

4) 完善的日志记录,将所有与后台进行通信的终端 IP 地址,通信时间,通信内容等记录到日志中,以供分析。

3 系统可靠性的实现

因为GPRS信号存在盲点,即有时可能会因无信号而中断网络传输。但金融服务系统有着非常高的可靠性要求,要求即使在无信号时也要保证数据的不丢失性。在ATM清机服务系统中,采取了以下两个措施来保证其可靠性:

1) 系统后台不保证发送的数据一定被PDA正确接收。一切数据接收及传送请求均由PDA发起,如PDA未能正确接收或发送数据,则需重新发起接收或传送请求。

2) PDA在通信失败时,将要发送的数据暂时保存起来,等信号好时,再将数据传给后台系统。

4 结语

文中的清机业务管理系统,已于2009年6月正式上线,至今已稳定运行9个多月,实现了ATM清机服务过程中的数据采集,远程信息查询,清机过程的实时监控,并为该金融服务公司和ATM所在银行提供了宝贵的经营决策支持数据(如加钞频率,故障率,卡钞率,钞箱管理数据等)。另外,该系统凭借其创新的设计及良好的应用前景在第十三届中国国际软件博览会上获得了创新奖。随着PDA应用在移动数据查询与采集领域越来越广泛,PDA与服务器端通信的效率,安全性,可靠性越来越重要,文中的方案对此类应用,具有比较大的参考价值。

参考文献(References):

[1] 汪诗锋,杨崇俊,刘冬林,等. 基于PDA的公共交通系统设计与实现[J]. 计算机应用研究, 2007,24(1): 280-282.
WANG Shi-feng, YANG Chong-jun, LIU Dong-lin, et al, Design and implementation of PDA-based public transportation[J]. System Application Research of Computers,2007,24(1): 280-282. (in Chinese)

[2] 王炫,唐靖寅 马蔚纯,等. 基于PDA的港口港政监督管理信息系统设计与实现[J]. 计算机应用与软件,2009,26 (5): 101-103.
WANG Xuan, TANG Jing-yin, MA Wei-chun, et al. Design and realization of information system of supervision and management for harbour governance based on PDA[J]. Computer Applications and Software, 2009,26(5): 101-103. (in Chinese)

[3] 郭雪莲,陈建勋,伍江华. 基于PDA的交通营运稽查管理系统[J]. 武汉科技大学学报:自然科学版,2004,27(1) :72-75.
GUO Xue-lian, CHEN Jian-xun, WU Jiang-hua. PDA-based traffic checking and management system[J]. Journal of Wuhan University of Science and Technology:Natural Science Edition, 2004,27(1) :72-75. (in Chinese)

[4] 孟德欣,谢二莲,金炎云. 一种基于GPRS的自定义数据帧传输系统的设计[J]. 计算机应用与软件,2009,26(2): 217-218.
MENG De-xin,XIE Er-lian,JIN Yan-yun. The design of a kind of data frame transmission system based on GRPS[J]. Computer Applications and Software,2009,26(2):217-218. (in Chinese)

[5] 姚振锋,张志鸿. 一种基于类ISO8583通信协议的数据交换格式[J]. 安阳工学院学报,2006 (1):52-54.
YAO Zhen-feng, ZHANG Zhi-hong. A modified ISO8583 protocol based on data exchange format [J]. Journal of Anyang Institute of Technology,2006(1):52-54. (in Chinese)

[6] 甄慕华,刘昌余,杨富富. 基于ISO8583的自助终端系统的设计与实现[J]. 湖南科技学院学报, 2009,30(4):118-122.
ZHEN Mu-hua,LIU Chang-yu,YANG Fu-fu. Design and realization of self-help terminal system based on ISO8583 protocol[J]. Journal of Hunan University of Science and Engineering,2009,30(4): 118-122. (in Chinese)

[7] 张裔智,赵毅,汤小斌. MD5算法研究[J]. 计算机科学,2008,35(7):295-297.
ZHANG Yi-zhi, ZHAO Yi,TANG Xiao-bin. MD5 algorithm[J]. Computer Science,2008,35(7): 295-297. (in Chinese)

[8] 蒋波. 一种基于三重DES和RSA的综合加密方案[J]. 微计算机信息,2007,23(18):52-53.
JIANG Bo. A encoding solutions based on triple DES and RSA[J]. Microcomputer Information,2007,23(18):52-53. (in Chinese)

(责任编辑:邢宝妹)