路桥收费系统实时模式和数据安全策略①

The Data Security and Real – time model of Highway toll system

侯济恭　(福建泉州 华侨大学信息科学与工程学院　362011)

摘要:路桥收费系统数据安全和保证交通畅通十分重要。数据安全含物理安全、数据操纵安全和人员操作安全,保证畅通同意味着系统必须实时运行。运用改进型的信号灯模式以及多缓冲池分布技术,黑匣子技术,再辅以自动多重备份等软硬件相结合技术,可以保证系统实时运行和数据安全。

关键词:实时　黑匣子　数据安全

1　数据安全与车道畅通

路桥收费系统的数据安全和保证交通畅通非常重要,它事实上是一个实时系统。路桥收费系统[1]由若干车道机(客户端)和服务器组成一个局域网,假定系统使用 C/S 模式,车道机每发出一张征费票据,必须将数据存入服务器的数据库中。为保证数据安全,通常的保存数据算法是:

(1) 形成一条收费记录 R

(2) if(数据库服务器连接成功)

将记录 R 写入数据库;

else

把记录 R 写入本地数据库;

(3) 结束

这种算法看起来很完美,但实际运行中却行不通。问题出在第 2 步,检测数据库服务器是否连接,如果发生服务器连接不上,比如网络断线,则每一步检测不论采用 C/S 或 SOCKET(TCP/IP)模式,系统需要耗时 5 秒左右,有时长达 1 分钟才有检测结论。这是因为用 Ado 连接服务器的数据库,系统默认的超时是 15 秒。采用 TCP/IP 协议传送数据,TCP 的作用是在发送与接收计算机系统之间维持连接,同时还要提供无差错的通信服务,将发送的数据报文还原并组装起来,自动根据计算机系统间的距离远近修改通信确认的超时值,从而利用确认和超时机制处理数据丢失问题,以便保证数据传送的正确性[2]。这个操作所花的时间也在 5 秒左右。虽然我们可以根据实际情况来设置超时时长,以加快系统响应时间,例如 ado 连接,

```
with AdoConnection1 do
begin
  ConnectionString := '';
  ConnectionTimeout := 5; //超时限制 5 秒
  Open;
end;
```

采用 socket 设置

```
int TimeOut = 5000; //超时限制 5 秒
setsockopt ( SockRaw, SOL _ SOCKET, SO _ RCVTIMEO,
(char *) &TimeOut,sizeof(int));
```

但这个时间是不能设置太短,否则,将引发其他类型的数据传送错误。因为每一次卖票过程要求在 5 秒内完成,一般将其设定为 10 秒。由于通信的故障,于是出现车道上排起一长串车,等待计算机响应现象,堵车现象十分严重,特别在交通高峰期,严重影响交通。

数据安全分为物理安全、逻辑安全和操作流安全,是系统的硬件配备、数据操纵方法和人员操作方式的结合。保证畅通就是使车道机为非一般意义的实时系统。寻找一种既能使数据安全,又不影响车道畅通的运行模式,就是本文所要讨论的问题。

2　系统结构

收费站服务器与车道计算机组成局域网,采用交

① 基金项目:福建省交通厅基金资助项目(福建省交通厅[2003]15 号文批准立项

互式以太网模式。由于服务器和车道之间距离大约100 米,且都是露天,为避免二次雷感应,车道机和服务器之间采用光纤连接。考虑到磁盘介质损坏对数据和系统崩溃可能对数据产生的影响,车道机和服务器的存储结构分别设计如图1 所示。

车道收费系统控制所有的车道设备。车辆到来时,自动抓拍图像,接受收费员的操作,显示收费金额,并进行语音报价,同时通过字符叠加器将金额、票号、征费员等信息叠加到监视图像;将数据写本地数据库,再写入本地缓冲池。缓冲池分为 A、B 两块,写入算法

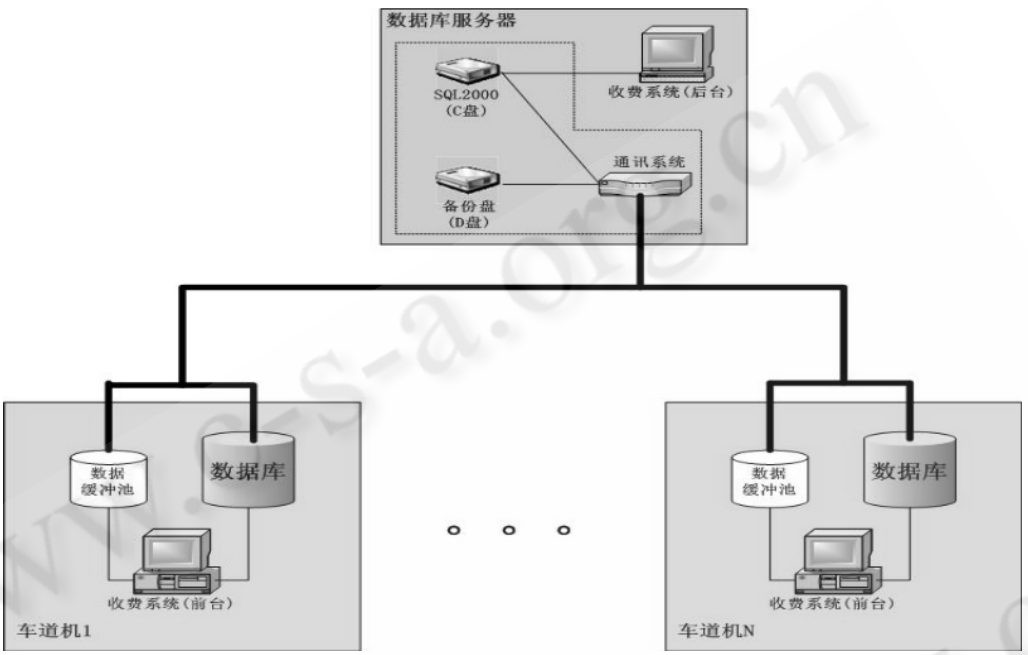

图 1　收费系统存储结构原理图

(1) 车道机系统设有收费数据库、数据交换池和操作流日志库。车道机首先将收费数据、操作流等数据存入本地硬盘上的数据库和操作流日志库,再将收费数据存入数据交换池。数据交换池用于与服务器中的通讯系统通信。车道机完全独立运行。

(2) 数据库服务器配备两块硬盘。C 盘作为SQL2000 数据库管理系统(主库),D 盘作为数据备份(备份库)。通信服务器定时向各车道机采集数据,将数据同时存放在两个物理盘。

由于收费数据存放在 3 个物理盘上,数据的恢复轻而易举,从而保证收费数据的物理安全性。

3　分布式数据交换

借鉴软件工程中 Agent 的概念,在服务器和车道机之间建立一个代理层,即通信器。该软件可以安装在任意一台的计算机,一般而言,它安装在数据库服务器计算机中。

是:

```
Flag = False ; //写数据库成功标志
  do {
  { if(缓冲池 A 状态 = = Idle )
    { 缓冲池 A 加锁;
      将数据写入缓冲池 A;
      缓冲池 A 解锁;
      Flag = True;
      }
  else
  if(缓冲池 B 状态 = = Idle)
    {缓冲池 B 加锁;
          将数据写入缓冲池 B;
          缓冲池 B 解锁;
          Flag = True;}
  } while (Flag = = False);
```

服务器端的通信器能够动态监测网络的工作状态,其采集各车道机数据的算法是:

```
if (缓冲池 A 状态 = =Idle)
  {缓冲池 A 加锁 ;
   do { 从缓冲池 A 读出数据 R;
        写入主数据库;
        写入备份数据库;
     } while (入库数据 ! = 缓冲池 A 数据);
  弹出冲池 A 数据;
  缓冲池 A 解锁;
  }
if (缓冲池 B 状态 = =Idle)
  {缓冲池 B 加锁;
   do {从缓冲池 B 读出数据 R;
        写入主数据库;
        写入备份数据库;
     } while (入库数据 ! = 缓冲池 B 数据);
  弹出冲池 B 数据;
  缓冲池 B 解锁;
  }
```

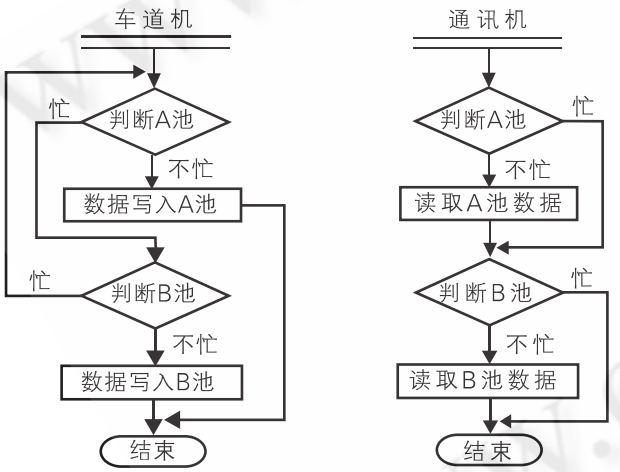

图 2　数据交换模式

通信器和车道机的数据交换模式见图 2,其关键是保证车道机具有抢先写数据的权利。由于通讯机一旦判断出缓冲池忙,马上放弃对它的操作要求,因此在任何时间点,通讯机至多只能占用一个缓冲池,这就保证车道机至少有一个缓冲池可以写入数据。另一方面,车道机只能占用一个缓冲池,因此也保证通讯机有采读数据的时间。由于采用通信器主动分布式采集数据方式,即通信器轮流向系统中的车道机收集数据,这样就避免系统中多并发进程,从而避免系统死锁。通讯机将所读数据写入数据库模拟数据事务处理,以保证数据的准确性和可靠性。

对于前台,实时要求严酷。对于后台,数据的实时性要求不高,延误几分钟不会影响系统的性能,其重点是数据传送的安全、可靠和准确。

4　计算机黑匣子

收费站发出的票据是有价证券,必须经得起稽核与查证。为保证每一张票据的准确可靠,票证号码在硬件(票号叠加在监控中)和软件(票号逐一自动核对)予以双重保险。但是在现实中,难免出现以下问题:打印机出故障,少出票或多出票;征费员对车型判断失误,例如 10 元车判断为 15 元车,导致错票;性急的操作,导致多出票等等。

以上的操作,通称为操作流失误。我们设计一个前台黑匣子,将操作员的每一个按键、发生的时间通通记录下来(图 3)。其结构是 BlackBoxP(操作时间,操作者、动作)。

```
2004 -10 -30 16:42:01  工号: 按键: + 上班
2004 -10 -30 16:42:09  工号: 110 操作:将票号[00000000]
改为[1178025],确认修改失败!!
2004 -10 -30 16:42:09  工号: 110 操作:将票号[00000000]
改为[1178026],确认修改失败!!
2004 -10 -30 16:42:12  工号: 110 输入票号为:1178175
2004 -10 -30 16:42:14  工号: 110 按键:5 (25 元)
2004 -10 -30 16:42:14  工号: 110 按键:回车
2004 -10 -30 16:42:15  工号: 110 操作:票号:1178175,
已售出。金额:25
```

图 3　前台黑匣子

实践证明,黑匣子对于数据错误的分析和追踪,对于数据的恢复,对于考评操作员的业务能力,具有很大的意义。

在程序设计上,为减少操作错误而产生的错票,保证输入一个车型选择只打印一张票据,操作流分 2 个事件处理。

选车型事件操作流:

(1) 选择车型

(2) 重复 1 直至按回车键确认

(3) 设定已选择车型状态;

确认事件操作流

if (已经选择车型 and 两选择车型事件时间差 < TimeOut)

{ 形成数据记录;打印票据;清除已选择车型状态;}

通常 TimeOut 设定为 1 ~ 3 秒。因为不可能在这么短的时间中内连续出售两张票据,所以在确认事件中作一个时间限制,这样就可以最大限度减少重复打票操作。但是,错票还是不可避免的,系统设计一个错票黑匣子,允许输入错票,错票黑匣子结构是:

ErrorFee(票号,售票日期时间,售票车道号,票面金额,售票员,修改日期时间,操作员,备注)错票的确认和录入是,每一张错票由当事人、当班班长和监控员签字,再由出纳录入错票表。算法要点是: 判断输入的票号是否在收费库中,是则有效错票,否则,拒绝接收。

当班收费员上缴收费款时,系统可以打印该收费员的日报表,含应缴金额,错票金额,应缴金额中自动扣除错票金额。

通过错误票据的对低方式,保证数据操作安全,从源头上遏制人为的侵吞票款行为。

由于前台工作很紧张,因此,有些票据的整理工作放在后台进行,这也需要建立一个后台操作黑匣子,忠实记录对票据的每一个操作。

5 车道计算机选择

车道计算机的性能是整个系统数据安全的基础,一般而言,选取计算机时考虑以下几个指标:

(1) 可靠性。计算机必须具有抗灰尘、油烟雾、震动、高低温、潮湿、电磁干扰等性能。MTTF 10 万小时以上(普通 PC 的 MTTF 仅为 10000 ~ 15000 小时)。如机箱采用钢结构;底板面积大;电源有较强的抗干扰能力等。

(2) 实时性。对车道现场进行实时在线检测与控制,对设备状况的变化给予快速响应,能及时进行采集和输出控制。

(3) 扩充性。具有多样 I/O 通道,能与现场的各种外设如与车道控制器、视频监控系统、车辆检测仪等相连。

(4) 兼容性。能同时利用 ISA 与 PCI 及 PICMG 资源,支持各种多媒体设备如视频捕捉卡、声卡等。并支持各种操作系统。

6 车道机与外设的通信

与车道机相连的外部设备很多,比如计重收费时的重量衡仪表,ETC 的 IC 卡读卡机、车辆感应器、字符叠加器等。通常这些设备都通过 RS232 与车道机交换数据。数据通信的第一个问题是传输距离。RS - 232C 标准规定:当误码率小于 4% 时,要求导线的电容值应小于 2500PF。对于普通导线,其电容值约为 170PF/M,则允许距离 L = 2500PF/(170PF/M) = 15M 。对于一般设备,如字符叠加器等是可以满足要求,但对于计重设备和 ETC 的读卡机,这一距离无法满足要求,因为为保证车快速通过,通常设备与车道机的距离约为 20M。我们采用超五类屏蔽线作为通信线,其的电容值约为 50pF/m 左右,允许距离 L = 2500pf / 50 = 50M,效果非常好。第二个问题是保证数据采集的正确性。除通信时采用 CRC 编码外,还采用冗余数据、多数判决法,即下位机每次通信重复发三次,主机对这三组数据判断,取相同的一组作为正确的数据。由于下位机与车道机一次交换的数据量很少,不足 128 个字节,因此重发三次对系统实时性影响可以忽略不计。

7 结束语

本文提出的改进型的信号灯模式以及多缓冲池技术保证系统运转在实时状态,结合分布存储结构、黑匣子技术和防范方法保证数据的安全可靠。所有算法和防范措施均已经全部实现,并且在泉州市公路局所有收费站得到成功的应用。

参考文献

1 侯济恭,多媒体路桥征费系统设计[J],计算机系统应用,1999,7 p50。

2 王建华译,TCP/IP 开发使用手册,机械工业出版社,1999,p19 - 30。

3 侯济恭,基于车重的路桥自动征费系统[J],计算机系统应用,2003,5 p56。