文章编号:1001 - 9081(2005)01 - 0165 - 03

一种基于 Petri 网通信协议的分析和验证

王 晶,樊晓桠,曹 清
(西北工业大学 计算机学院,陕西 西安 710072)
(wangjingbox@yahoo.com.cn)

摘 要:基于一个 PDA 项目,介绍了自行设计的利用固定电话网进行信息传输的一套通信协议。用 Petri 网抽象描述了一系列代表性链路层协议模型,并借助 Petri 网模拟工具对模型进行修正和改进,得到可实际工程应用的协议模型。

关键词:Petri 网;通信协议;冲突;协议验证
中图分类号: TP393.04 **文献标识码**:A

Analysis and validation of communication protocol based on Petri Net

WANG Jing, FAN Xiao-ya, CAO Qing
(Institute of Computer Science, Northwest Polytechnical University Xi'an Shaanxi 710072, China)

Abstract: Based on a PDA project, a communication protocol which communicated through PSTN was introduced. Then, a series of representative link layer protocol models using Petri net were described abstractly. By the direction of Petri net emulation tool, these models were modified and improved gradually. Finally, a protocol model which could be applied in the practical work was achieved.

Key words: Petri Net; communication protocol; conflict; protocol validation

0 引言

在本文描述的系统环境中,PDA 通过 PSTN 与测量中心和服务器进行数据交互。由于实际的物理设施限制,系统的工作方式是半双工的。并且考虑到开发过程中存在的限制,我们自行设计并实现了一个固化信息传输通信协议,它相对简单并且对本系统来说很合体。

系统采用的网络结构是简单的客户/服务器模式。根据实际线路的特点,本系统的通信协议层的划分相对简单许多,是由物理层、链路层和应用层三层组成。

(1) 物理层规定了电气特性和电路接口、链路建立的初期使用 DTMF 信号及链路建立完成后的信息交互使用 FSK 信号并为数据链路层提供服务;

(2) 链路层进行数据包的组包和解包、在 PDA 和服务器之间建立和释放数据链路、PDA 和服务器之间交互进行时序控制、数据传送进行出错处理、出错传送的重发处理并具有 FSK 上传的 PDA 的支持功能;

(3) 消息层下传以及上传 FSK 消息包中消息内容域的格式并规定 DTMF 命令响应的格式。

整个通信模块中的核心所在是链路层自定义的通信协议的设计和实现。只有在协议实现前进行充分的形式化描述、验证和实现之后的一致性测试,进一步的实现才是有保证的。文中接下来将详细讨论这一过程。

因为 PDA 与服务器的通信是半双工的。PDA 必须在接收到服务器的应答后才能进行下一个命令的发送,挂机命令除外。也就是说,这是一种"一去一回"的方式,比较简单。但没必要对每一次正确传输的数据包都回传一个链路层的响应,而只对出错的帧发响应信号。若校验正确,就接着看服务器或者 PDA 是否有信息要发送给对方,若没有信息则向对方发送一个链路层响应正确信息,如果有信息内容需要发送,则直接发送信息至对方而不需要再次发送链路层响应正确的数据包。从图 1 所示时序图可以看到这种"一去一回"的交互方式的工作。这种方法可以降低整个通信系统的复杂度,同时流程更加的明朗化,便于以后系统的扩充和更改。

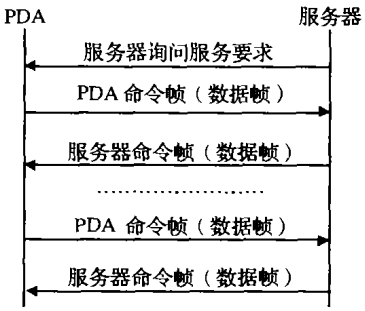


图 1 "一去一回"时序图

1 协议的 Petri 网模型

Petri 网是从 Carl Adam Petri 的早期(1962 年)工作发展起来的。30 多年来,Petri 网理论涉足许多领域,在计算机系统的设计和操作、通讯规程等方面得到了广泛而深入的应用。

使用 Petri 网作为协议定制的理论指导,我们首先基于通信过程中提出的"一去一回"的交互方式提出一个简单的

收稿日期:2004 - 07 - 09

作者简介:王晶(1980 -),女(蒙古族),宁夏人,博士研究生,主要研究方向:计算机科学与技术; 樊晓桠(1962 -),男,教授,博士生导师,主要研究方向:计算机 VLSI 系统设计、电子设计自动化; 曹清(1979 -),男,湖南人,硕士研究生,主要研究方向:数据通讯与计算机网络.

Petri 网模型 1,在进一步分析验证后找到了更加合理适用的 Petri 网模型 2 和 3。

从上述 PDA 与服务器之间的交互的时序图中可以进一步看出,从发送端来看,它总是需要等待数据接收端的回应信息。即使接收端回送的信息不符合下一步行为的操作,此时认为数据帧发送失败,只需要重新发送前一数据帧。由此,如果不管发送双方的发送内容,只讨论发送对象发送的时序关系,因此我们可以把自定义的链路层通信协议看作是一种停止-等待协议。建立 Petri 网模型 1(一般的停止-等待协议模型)如左图 2 所示。图中 Pi 表示发送方,信道和接收方所处的状态(库所),Ti 表示状态的变迁,K≡ω,W≡1 即所有库所之容量均为无穷,所有弧上的权均为 1,初始标识如图所示(1,0,0,1,1,0,0,0),简称为(1,4,5)。模型 1 中各个库所和变迁的意义如下:(1)库所说明:P1:发送方等待第 1 帧的回应,P2:发送方等待第 2 帧的回应,P3:接收方等待第 2 帧,P4:接收方等待第 1 帧,P5:第 1 帧在信道中,P6:第 1 帧的回应在信道中,P7:第 2 帧的回应在信道中,P8:第 2 帧在信道中。(2)变迁说明:T1:发送方发送第 1 帧,T2:发送方发送第 2 帧,T3:接收方收到第 1 帧,T4:接收方收到第 2 帧。

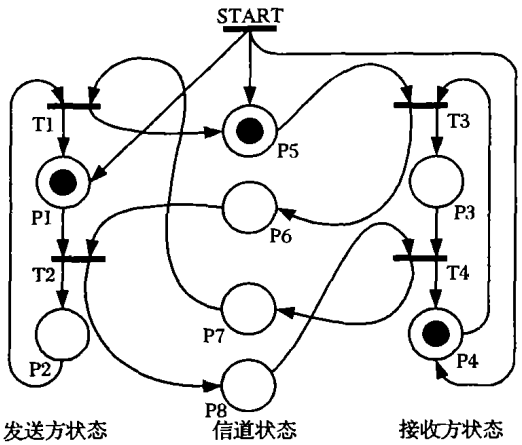


图 2 Petri 网模型 1

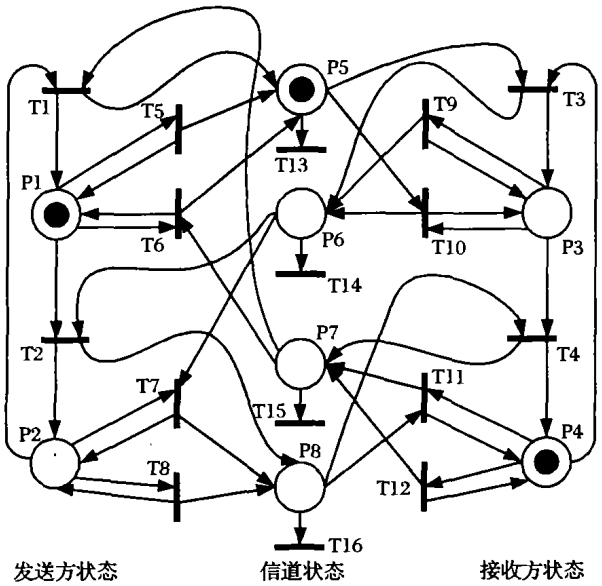


图 3 Petri 网模型 2

一般的等-停模型中,抽象的基础是认为通信信道比较畅通。但本系统应用的传输介质是公用电话网,通信状况较差。因此必须在协议中引入超时与出错双重处理的机制。这时,当发送方与接收方收到与所处状态不符的数据帧时,发送上次所发出的帧。引入这两种机制后,我们得到了模型 2。它的库所和变迁意义为:(1)库所说明:同模型 1。(2)部分变迁说明:T1:发送方发送第 1 帧,T3:接收方发送第 1 帧回应,T4:接收方发送第 2 帧回应,T5:发送方等待第 1 帧回应超时,T6:发送方等待第 1 帧回应时,却收到第 2 帧的回应,T10:接收方等待第 2 帧时,却收到第 1 帧,却收到第 2 帧,T13:第 1 帧丢失,T14:第 1 帧回应丢失。

2 冲突的检测

在半双工的通信模型中,信道状态中同时最多只能有一个 token,否则会造成多组信号在信道内叠加,而造成参与通信的双方都收到脏数据。这种情况下,接受方无法处理,而反复要求对方重发,降低了通信信道的利用率,增加了通信时间。

因此该模型需要遵守一个重要的约束条件:

$$\sum m_i \leqslant 1$$

其中 m_i 为信道某时刻信道库所中的 token 数。它的意思是任一时刻,信道中的所有 token 数目之和为 0 或 1。如果某一时刻,出现 $\sum m_i > 1$ 的情况,则认为有冲突发生。

我们使用了 SimPRES 对 Petri 网模型 2 进行模拟以检测冲突的发生。SimPRES (a Simulator of Petri net based Representation for Embedded Systems),是一种嵌入式系统的 Petri 网模拟工具,相比于其他 Petri 网工具,SimPRES 为 Petri 网增加了变迁的时延的扩展。其中,设定每一个变迁的最小变迁时延(minimum transition delay) d_i^- 和最大变迁时延(maximum transition delay) d_i^+,单位为秒,且有 $d_i^- \leqslant d_i^+$。除了所有的超时变迁 T5,T8,T9 和 T12 外,设定其他变迁 $d_i^- = 0$, $d_i^+ = 1$,其变迁点火策略(firing policy)服从均匀分布。设定四个超时变迁的 $d_i^- = 0$, $d_i^+ = 5$,其点火策略为尽可能延迟。所以,变迁的触发时间(trigger time),即变迁的点火时间,就由 d_i^-、d_i^+,以及点火策略决定。

用 SimPRES 模拟 100 次,每次的总时间为 100 秒(经过在实际线路上验证,一次正常传输平均需要 1 分半,也就是 100s),记录每次冲突发生的总的次数,即不满足条件($\sum m_i \leqslant 1$)的次数。发现出现冲突的次数在 1~30 之间,部分模拟结果见下表 1。在这种情况下无法进行正常的通信。因此,我们必须进一步修改模型 2 来减少信道中的数据冲突。需要注意的是,如果在模拟中将超时变迁的设置改为和上述其他变迁相同的值,而不修改点火策略(仍然是尽可能延迟),经过模拟后发现冲突依旧存在。说明超时的延迟时间的长度非常关键,它会影响到整个通信过程的畅通与否。测试前期所做的超时延迟时间长度的假设都是不可靠的。只有在真实的通信环境下的严格测试,才能确定一个较好的延迟时间值设定。才能进行更加贴近真实状况的测试。

3 Petri 网模型的进一步改进

从上文可以看出对模型 2 的修改非常必要。通过对冲突

的观察以及对时序图的分析发现,症结所在是因为双方都有超时重发机制。例如某帧丢失,接受方等待超时,发送应答帧询问,同时发送方可能因为没有收到应答帧等待超时所以重发帧。这样很有可能造成应答帧和重发帧同时在信道中而引起冲突。因此我们放弃了对称超时策略(即发送方和接收方都有超时机制),而采用非对称超时策略。也就是发送方做超时重发,而接收方不重发,当接收方收到上一帧的时,表明是发送方重发的帧,接收方则简单的回应上一帧就行了。在经过修改后得到非对称的 Petri 模型 3 如上图 4 所示。其中库所和变迁的意义如下:(1)库所说明:同模型 1(2)变迁说明:T1 ~ T6 同模型 2,T7:接收方等待第 2 帧时,却收到第 1 帧,T9:第 1 帧丢失,T10:第 1 帧回应丢失。

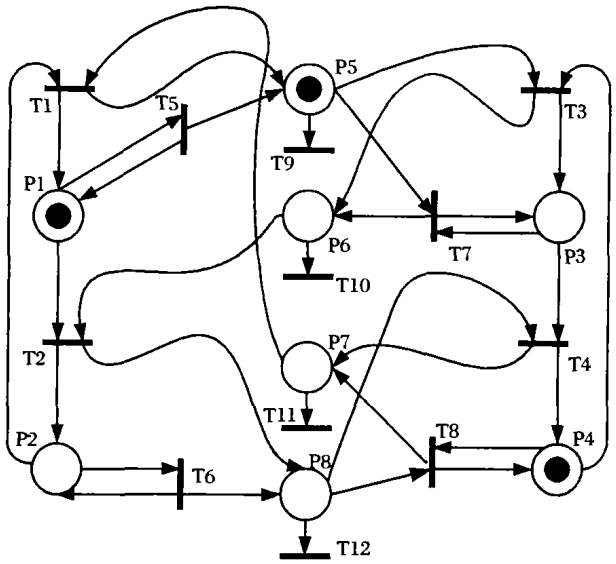


图 4　Petri 网模型 3

在同样的设置条件下用 SimPRES 进行模拟。部分测试结果如下表 1。可以看到冲数目全都为零。证明经过修改后模型 3 在通信过程中可以保证不会发生两个数据帧同在信道中的情况。这就是说,它满足约束条件($\sum m_i \leqslant 1$)。此外,由于模型 3 是从 1 模型 1、2 逐渐演变过来的,所以它具有等-停协议的简单而便于实现的特性,同时还具有超时和出错重发的机制。因此模型 3 我们经过修正和改进,最后得到的可实际工程应用的协议模型。

表 1 SimPRES 的模拟结果

次数	模型 2	模型 2
1	14	0
2	25	0
3	16	0
4	12	0
5	25	0

4　协议认证

· 由图 4 以及 Petri 网基本知识可得模型 3 的关联矩阵 C 如下:

$$C = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

其矩阵元素 $C(P_i, T_j) = W(T_j, P_i) - W(P_i, T_j)$。

· S_不变量

通过计算得出 S_不变量为 $X_1^T = (1, 1, 1, 1, 0, 0, 0, 0)$, $X_2^T = (1, 1, 0, 0, 0, 0, 0, 0)$, $X_3^T = (0, 0, 1, 1, 0, 0, 0, 0)$。$X_1 = X_2 + X_3$,因为 X_2, X_3 相互独立,所以 X_2, X_3 代表模型 4 中若干个资源的流动范围,即它中包含的 token 个数的和在任何可达标识之下都不变。

· T_不变量

通过计算得出 T_不变量为 $X_1^T = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$。说明所有从初始标识出发的 $M_0 = (1, 0, 0, 1, 1, 0, 0, 0)^T$, Petri 网模型 3 都能回到系统初始标识。

· 有界性

通过计算得 $K = 1$,但是因为该 Petri 网模型不是基本网系统,所以 $K = 1 + 1 = 2$。

· 活性、完整性、前进性和终止性

我们可以方便的画出模型 3 的可达图。由于任何一个变迁都存在某个标识下发生,所以网是活的,协议是无死锁的。此外,协议所描述的状态都是可以达到的,而且其中没有无用循环的,其最终状态总是回到初始状态。

5　结语

本系统考虑到项目的实际情况,设计了简单实用的三层模型。经过不断的抽象和分析,得到了最终适用的通信协议模型,并进行了较为完善的协议认证。最终在我们定义的链路层协议中规定了如下三个方面的内容:(1)各种帧格式。它和本文讨论问题无关不详述;(2)PDA 和服务器之间的交互通信。包括建立呼叫链路、身份认证、数据传送(包含 PDA 下载信息和 PDA 信息上传)、连接释放;(3)重发机制:包含超时重发和出错重发,重发 3 次后,仍然不正确,断开链路,挂机。在完成抽象分析的基础上,我们在 Linux 平台的开发环境上,实现了整套通信协议,很好的满足了用户的需求。

参考文献:

[1] 袁崇义. Petri 网原理[M]. 电子工业出版社, 1998.

[2] HOLZMANN G. Design And Validation of Computer Protocols[M]. Pearson Education POD Facsimile edition, 1990.

[3] RUSSELL T. Telecommunications Protocols [M]. 2 nd Edition. McGraw-Hill Professional Publishing, 1999.

[4] TANENBAUM AS. Computer Networks[M]. Fourth Edition. Prentice Hall, 2003.

[5] ESSER R, TEICH J, THIELE L. CodeSign: An Embedded System Design Environment[J]. IEE Proc. Computers and Digital Techniques, 1998, 145(3):171 - 180.