一种兼顾协议正确性验证和性能评估的 Petri 网方法*)

范 昊[1,2] 吴哲辉[2] 曾庆田[2]

(中国科学院计算技术研究所智能信息处理开放实验室 北京 100080)[1]

(山东科技大学信息与工程学院 青岛 266510)[2]

摘 要 基于 Petri 网的协议形式化分析方法由于其精炼、简洁和无二义性逐步成为分析协议的一条可靠和准确的途径,但是协议的形式化分析目前研究还不够深入,协议分析的两个重点内容正确性验证和性能评估所需要的模型不同,一种模型只能解决一方面的工作。为了有效地解决这一问题,文中提出了一种用原型 Petri 网作为协议验证模型的思路和方法,在不改变原型 Petri 网结构的基础上对变迁赋予发生时延,解决了协议的性能评估问题。本文还给出了协议验证内容与 Petri 网分析方法的对应关系,并对 0-1 停止等待协议进行了详细的分析,最后把 0-1 停止等待协议的原型 Petri 网模型转化为时延 Petri 网,对协议的性能进行了评估。

关键词 协议验证,形式化分析,时延 Petri 网,协议性能评估,0-1 停止等待协议

Protocol Validation and Performance Evaluates Based on Petri Nets

FAN Hao[1,2] WU Zhe-Hui[2] ZENG Qing-Tian[2]

(Opening Laboratory of Intelligent Information Processing, Institute of Computing Technology Chinese Academy of Sciences, Beijng 100080)[1]

(College of Information Science and Engineering, Shandong University of Sciences and Technology, Qingdao 266510)[2]

Abstract Formal methods for the analysis of protocol based on Petri nets have been looked on a credible and exact way in protocol analysis. But now, the research on formal analysis of protocol is not thorough. Particularly, there is some conflict between protocol validation and evaluates. In this paper, we make a summary of the methods on protocol analysis based on Petri nets. Then we investigate the relationship between the protocol behavior and the properties of Petri nets. The most important is that we propose a new method about protocol analysis. This method gives a detail validation of protocol using prototype Petri net. We change prototype Petri net into Timed Petri net, so the protocol performance evaluates problem can be solved. As an example, we make a detail analysis of 0-1 stop-and-wait protocol using Petri nets model and give evaluates the performance of it using TPN.

Keywords Protocol validation, Formal analysis, Timed Petri Net, Protocol performance evaluates, 0-1 stop and wait protocol

随着网络服务要求的提高,网络系统的复杂性在协议方面体现出空间分布性、并发性、异步性、不稳定性和多样性。在这种情况下,需要合适的方法、技术和计算机辅助工具来对协议进行正确性验证和性能评估[1,2]。对协议本身的逻辑正确性进行校验的过程称之为验证[3]。协议的正确性验证试图在协议具体实现前最大限度地检测和纠正协议错误和缺陷,包括死锁、活锁、错误的动作序列,接收或发送缓冲区的溢出,遗漏或重复接收报文等等。协议的性能评估主要是对协议的吞吐量、数据的传送时延等指标的评价,性能评估对协议的服务质量(QoS)有着重要的影响,是目前网络研究的热点问题之一。

基于 Petri 网的协议形式化分析方法由于其精炼、简洁和无二义性逐步成为分析协议的一条可靠和准确的途径[4]。许多方面的研究都取得了一定的成果,如在协议的正确性验证方面,东南大学提出的 Epr/TN 系统在谓词/变迁网的基础上增加了禁止弧和删除弧以描述协议中的零检测能力和异或运算,该方法已应用于差错恢复协议的建模和验证[5]。文[6]中利用颜色 Petri 网模型对 OSPFv3 协议进行了分析,对复杂的协议建立了层次模型,对模型加入了事件驱动机制。对协议性能评估的研究主要有以下几种形式化分析方法,柏林工业大学的 Christian Kelling 等人利用随机 Petri 网为几种著名的令牌协议建模,除了分析系统的确定性行为之外,还根据不同的优先级分别进行了传输特性的性能评价[7]。清华大学的林闯教授应用随机 Petri 网,结合马尔可夫链模型分析了 ATM 协议的性能特征。山东科技大学的张广胜及其导师吴哲辉教授利用时间 Petri 网对 A-D 协议进行了详尽的分析,并引入复杂度矩阵对协议进行了性能评估[8]。

虽然很多协议的 Petri 网分析方法已经取得了丰硕的成果,然而很多方法在协议的正确性验证和性能评估方面存在着矛盾。良好的正确性验证模型不能方便地对协议性能做出定量的分析,良好的性能评估模型不能准确地反映协议的各种静态特征和动态行为。如果这一问题不能解决,当既要对协议的正确性验证又要对协议的性能评估时,必然造成对同一种协议建立多种 Petri 网分析模型的重复性工作。

为了更好、更有效地分析协议,本文提出图形化的、形式化的和易于用软件实现的分析模型—原型 Petri 网来解决协议正确性验证中存在的一些问题。然后对原形 Petri 网的变迁赋予发生时延,可以方便地将模型转化为时延 Petri 网并对协议进行性能评估。该方法可以充分利用 Petri 网已取得的理论成果,对协议进行验证,同时在不改变模型结构的基础上对变迁赋予时延,解决了对协议的性能评估的问题。本文将给出 0-1 停止等待协议的 Petri 网模型,并利用 Petri 网的各种分析方法对 0-1 等待协议进行全面的、综合的分析,最后对原形 Petri 网的变迁赋予发生时延,方便地将模型转化为时延 Petri 网并对 0-1 停止等待协议进行性能评估。

*)基金项目:国家自然科学基金资助课题(60173053)。范 昊 博士研究生,研究方向为 Petri 网理论及应用;吴哲辉 教授,博士生导师,主要研究方向为 Petri 网理论及应用、算法设计与分析等。

1 原型 Petri 网和时延 Petri 网的基本概念

定义 1[9] 一个原型 Petri 网系统可以定义为一个四元组$\sum=(P,T,F,M)$，其中

1)$P\cup T\neq\Phi$;2)$P\cap T=\Phi$;3)$F\subseteq((P\times T)\cup(T\times P))$;4)$dom(F)\cup cod(F)=P\cup T$; 5)$M: P\to\{0,1,2,\cdots\}$。

P 和 T 是两个不相交的集合，称为原型 Petri 网$\sum$的基本元素集，P 的元素称为 P 元或库所 Place，T 的元素称为 T 元或变迁(transition)。F 是网$\sum$的流关系，$dom(F)$和 $cod(F)$是 F 前域和后域。M 称为网$\sum$的一个标识。

定义 2[9] 原型 Petri 网$\sum=(P,T,F,M)$有如下变迁发生规则

1)对 $t\in T$，若$\forall p\in{}^{\cdot}t: M(p)\geqslant 1$，称 M 授权 t 发生，记为 $M[t>$。

2)若标识 M 授权 t 发生，则变迁 t 在 M 下可以发生，从 M 发生 t 得新的标识 M'(记作 $M[t>M'$)，对$\forall p\in P$:

$$M'(p)=\begin{cases}M(p)-1 & \text{当 } p\in{}^{\cdot}t-t^{\cdot}\\ M(p)+1 & \text{当 } p\in t^{\cdot}-{}^{\cdot}t\\ M(p) & \text{其他}\end{cases}$$

定义 3[9] 设$\sum=(P,T,F,M)$为一个 Petri 网，$P=\{p_1,p_2,p_3,\cdots,p_m\}$，$T=\{t_1,t_2,\cdots,t_n\}$，则 Petri 网$\sum$的结构$(P,T;F)$可以用一个 n 行 m 列矩阵$A=[a_{ij}]_{n\times m}$来表示。其中

$a_{ij}=a_{ij}^{+}-a_{ij}^{-}\quad i\in\{1,2,\cdots,n\},j\in\{1,2,\cdots,m\}$。

$$a_{ij}^{+}=\begin{cases}1 & \text{当}(t_i,s_j)\in F\quad i\in\{1,2,\cdots,n\},j\in\{1,2,\cdots,m\}\\ 0 & \text{否则}\end{cases}$$

$$a_{ij}^{-}=\begin{cases}1 & \text{当}(p_i,t_j)\in F\quad i\in\{1,2,\cdots,n\},j\in\{1,2,\cdots,m\}\\ 0 & \text{否则}\end{cases}$$

称 A 为$\sum$(或网 $N=(P,T;F)$)的关联矩阵(incidence matrix)。

定义 4[9] 设$\sum=(P,T,F,M_0)$为一个 Petri 网，$s\in S$，若存在正整数 B，使得$\forall M\in R(M_0): M(s)\leqslant B$，则称库所 s 为有界的(bounded)，并称满足此条件的最小正整数 B 为库所 s 的界，记为 $B(s)$。即

$$B(s)=\min\{B\mid\forall M\in R(M_0): M(s)\leqslant B\}$$

当 $B(s)=1$ 时，称库所 s 为安全的。

定义 5[9] 设$\sum=(P,T,F,M_0)$为一个 Petri 网，如果每个 $s\in S$ 都是有界的，则称$\sum$为有界 Petri 网。称 $B(\sum)=\max\{B(s)\mid s\in S\}$为$\sum$的界。当 $B(\sum)=1$ 时，称$\sum$为安全的。

定义 6[9] 设$\sum=(P,T,F,M_0)$为一个 Petri 网，$t\in T$。若对任意$\forall M\in R(M_0)$，存在 $\sigma\in T^{*}$，使得 $M[\sigma>M'$且 $M'[t>$，称 t 为活的。如果一个 Petri 网中的每一个变迁都是活的，则称这个网是活的。

定义 7[9] 设 $N=(P,T;F)$为一个网，$|P|=m$，$|T|=n$，A 为 N 的关联矩阵。

1)如果非平凡的 m 维非负整数向量 Y 满足 $AY=0$，则称 Y 为网 N 的一个 P-不变量。

2)如果非平凡的 n 维非负整数向量 X 满足 $A^{T}X=0$，则称为 X 网 N 的一个 T-不变量。

定义 8[9] 设 Y 和 X 分别为网 $N=(P,T;F)$的 P-不变量和 T-不变量。记

$\|Y\|=\{p_j\in P\mid Y(j)>0\}$

$\|X\|=\{t_i\in T\mid X(j)>0\}$

并分别称它们为 p-不变量 Y 的支撑集和 T-不变量 X 的支撑集。

定义 9[8] 时延 Petri 网是一个五元组：$TPN=(P,T,F,\tau,M)$其中 P,T,F 同定义 1 中的含义相同。τ 是时间映射函数$\tau\to 0\cup Q^{+}$(Q^{+}为正有理数)。规定网中每个变迁的持续时间。当持续时间为 0 时称为瞬时变迁，不为 0 是称之为时延变迁。$M: p\to\{0,1,2,\cdots\}$是网系统的标识。

有关 Petri 网的其他概念和定理请参阅文[9,10]。

2 协议的正确性验证和性能评估的 Petri 网方法

表 1 协议验证内容与 Petri 网分析方法对照表

协议验证内容	Petri 网分析内容	Petri 网分析方法
协议状态之间的可达关系	可达性分析	有界 Petri 网的可达标识图
死锁	Petri 网的活性，死锁、陷阱理论	有界 Petri 网的可达标识图
协议中某些参数（通道，缓冲区）是否有界	有界性	Petri 网的结构有界性理论和库所子集结构有界的充要条件
在协议的运行过程中部分参数是否守恒	P-不变量	有界 Petri 网的 P-不变量和守恒性理论
协议的动作序列是否可持续执行	T-不变量	有界 Petri 网的 T-不变量和协调性理论
协议的动作序列是否合法	Petri 网变迁发生序列	有界 Petri 网的可达标识图

2.1 协议正确性验证

协议的许多概念可以用 Petri 网模型来表达，而且 Petri 网的许多特性在协议中也可以找到实际的物理意义。表 1 简要地给出了二者之间的对应关系。

(1)静态分析

静态分析主要是分析协议的结构特性：结构活性、有界性、守恒性、安全性、P-不变量，T-不变量等。例如 P-不变量意味着协议的资源(数据帧，应答帧)守恒。通过分析 Petri 网的拓扑结构特性，我们可以对协议的诸多性质进行分析，并由此验证协议的正确性。

(2)动态分析

分析协议的动态性质如执行的动作序列、可达性、活性等。给定 Petri 网的初始标识，按照 Petri 网的可达图标识图构造算法，可以得到 Petri 网的可达标识图。Petri 网的可达图含有一些对验证协议正确性非常有用的信息，它可以分析协议状态的可达性(从一个状态到另一个状态)、执行序列、协议错误状态的可恢复性等。

2.2 协议性能评估

正确性是协议的最基本的条件，然而它的效率和吞吐量(throughput)、数据传送时延等也是实际应用中必须考虑的重要问题，特别是对通信实时性要求较高的协议(如视频传输，语音传输等)。现有的协议形式化分析都很少涉及这一问题，时间 Petri 网能够有效地分析协议延迟时间和吞吐量等问题。对原型 Petri 网中的定义变迁发生的延迟时间，就可以将原型 Petri 网转化为时延 Petri 网，对时延 Petri 网构造其可达标识图就可以实现对协议性能的评估，这也是本文的优越性所在。本文主要考虑以下两个指标。

(1)最大吞吐量

每秒成功发送的最大数据帧数就是链路的最大吞吐量，记为 λ_{max}。

(2)平均传播时延

正确传送一个数据帧所需的平均时间，记为 t_{AV}。

3 一个实例：0-1 停止等待协议

3.1 0-1 停止等待协议简介

在停止等待协议中发送端对出错的数据帧的重发是自动进行的，所以应用这类差错控制体系的协议又被称为自动请求重发 ARQ(Automatic Repeat request)协议。停止等待协议是最简单但也是最基本的数据链路层协议，其原理可以应用到网络协议的其他各层。对停止等待协议进行完整的形式化验证和性能评估具有重要的意义。

下面给出 0-1 停止等待协议的算法：

发送接点：

(1)从主机取一个数据帧。

(2)V(S)=0。{发送状态变量初始化}

(3)N(S)=V(S)；{将发送状态变量的数值写入发送序号}

将数据送交发送缓冲区。

(4)将发送缓冲区的数据帧发送出去。

(5)设置超时定时器。{选择适当的超时重发时间 t_{out}}

(6)等待。{等待以下三个事件中的其中一个}

(7)若收到确认帧 ACK，则：

从主机取一个新的数据帧；V(S)=1−V(S)；{更新发送状态变量，变为下一个序号}

转到(3)。

若收到否认帧 NAK，则：转到(4)。

{NAK 表示接收方检测出数据错误，请求重发数据帧}

若超时定时器时间到，则：转到(4)。

{超时的原因可能是发送方的数据帧在信道中丢失或是接收方的应答数据帧 ACK/NCK 丢失。}

接收接点：

(1)V(R)=0。{接收状态变量初始化，其数值等于欲接收的数据帧的发送序号 N(S)。}

(2)等待。

(3)当收到一个数据帧，就检查有无产生传输差错。若无差错，则执行(4)，否则转到(8)。

(4)若 N(S)=V(R)，则执行(5)。{收到发送序号正确的数据帧。}

若 N(S)≠V(R)，则丢弃此数据帧，然后转到(7)。

(5)将收到的数据帧送主机。

(6)V(R)=1−V(R){更新接收状态变量，准备接收下一个数据帧。}

(7)发送确认帧 ACK，并转到(2)。

(8)发送否认帧 NAK，并转到(2)。

3.2 0-1 停止等待协议的原型 Petri 网模型

给出 0-1 停止等待协议的原型 Petri 网模型如图 1，图 1 符号的说明如表 2。

表 2 图 1 中的符号说明

符号名称	库所/变迁含义	符号名称	库所/变迁含义	符号名称	库所/变迁含义
P_1	等待 ACK	P_8	ACK 或数据帧丢失	t_7	[1]帧丢失
P_2	等待 ACK	t_1	收 ACK 发[0]帧	t_8	收[0]帧不送主机
P_3	[0]帧在信道中	t_2	收 ACK 发[1]帧	t_9	收[1]帧不送主机
P_4	ACK 在信道中	t_3	[0]帧超时重发	t_{10}	收[0]帧送主机
P_5	[1]帧在信道中	t_4	[1]帧超时重发	t_{11}	收[1]帧送主机
P_6	期望收[1] 帧	t_5	[0]帧丢失		
P_7	期望收[0] 帧	t_6	ACK 帧丢失		

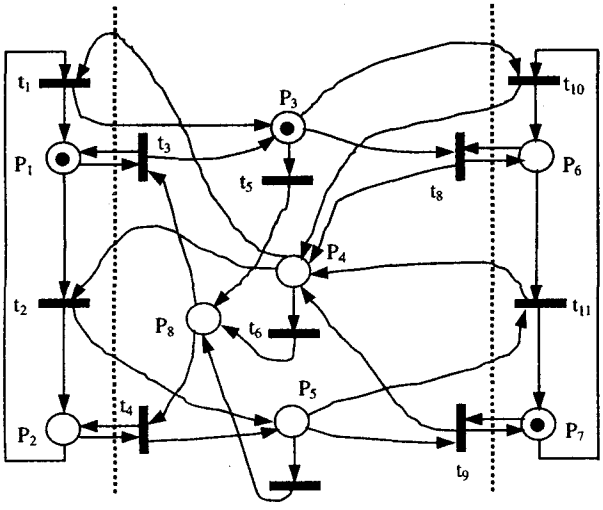

图 1 0-1 停等协议的 Petri 网模型

图 1 中的 P_8 表示信息的丢失，信息丢失有三种情况：a. [0]帧丢失。b. [1]帧丢失。c. ACK 丢失。图 1 中对这三种情况都不加区别地用库所 P_8 表示，这并不影响对协议的分析。

图 1 中没有对否认帧 NAK 加以描述，NAK 是在接收方发现接收到的数据有错误时回复给发送方的信号，接收方在此时要准备重新接收出错的数据帧。发送方在收到 NAK 后将重发上次发过的数据帧。这种情况与数据帧在通信信道中丢失的情况很相似，对 NAK 的分析可以等同于数据帧丢失情况的分析。

图 1 中 Petri 网的初始标识为：M_0=[1,0,1,0,0,0,1,0]，初始标识表明协议处于这样一种状态：发送方主机已经将 N(S)=0 的[0]号数据帧发送出去，并等待接收方的 ACK 信号。信道正处于传送[0]号数据帧的状态。接收方主机正处于期望接收[0]帧的状态。不失一般性，可以将此标识当作协议的初始状态。

3.3 0-1 停止等待协议的静态分析

首先给出 Petri 网模型的关联矩阵 A，关联矩阵可以对 0-1 停止等待协议进行以下各种静态分析和验证。

(1)P-不变量对协议守恒性验证

由 3.1 节给出的 0-1 停止等待协议的算法可知，如果将发送数据帧和接收数据帧的过程看作是瞬时的(包括发送和接收 ACK)，如果协议是正确的，发送方主机总处于这样一种状态：已发完[0]帧等待 ACK 或是已发完[1]帧等待 ACK。接收方主机总处于这样一种状态：期望收[0]帧或期望收[1]帧。信道总处于这样一种状态：正在传送[0]帧或正在传送

[1]帧或正在传送 ACK 或信号丢失。对应于图 1 中的 Petri 网模型，如果协议满足上述条件，那么描述发送方状态的库所子集$\{p_1, p_2\}$，描述接收方状态的库所子集$\{p_6, p_7\}$，描述信道状态的库所子集$\{p_3, p_4, p_5, p_8\}$都应该是 P-不变量的支撑集。

由方程 AY=0 可以得到解如图 2。从方程的解可以看出 0-1 等待协议是符合 P-不变量验证的。

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

$$\begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \\ Y_7 \\ Y_8 \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

图 2　关联矩了阵 A 和方程 AY=0 的解

(2)T-不变量对协议可持续执行的验证

由方程 $A^TX=0$ 可以得到：$\{t_5, t_3\}$，$\{t_6, t_3, t_8\}$，$\{t_{10}, t_2, t_{11}, t_1\}$都是 T-不变量的支撑集。T-不变量反应了 Petri 网模型循环子系统，所以$\{t_5, t_3\}$不变量支撑集反应了如下实际意义：[0]数据帧在信道中丢失，发送方在等待 ACK 一段时间后由于超时定时器超时将自动重发[0]帧。$\{t_6, t_3, t_8\}$不变量支撑集反应了系统在丢失 ACK 后的可恢复性。$\{t_{10}, t_2, t_{11}, t_1\}$不变量支撑集反映了系统可以成功地循环执行如下动作序列：发送[0]帧，收[0]帧发ACK，发[1]帧，收[1]帧发ACK。当然还有其他的 T-不变量的支撑集，这里不再赘述。

T-不变量验证说明了 0-1 等待协议具有错误状态的可恢复能力和持续发送数据帧的能力。

3.4　0-1 停止等待协议的动态分析

首先给出图 1Petri 网模型的可达标识图，如图 3，可达标识图可以对 0-1 停止等待协议进行以下各种动态分析和验证。

(1)协议发送、接收及信道有界性的验证

在 0-1 停止等待协议中，数据帧交替使用[0]/[1]编号，所以接收和发送缓冲区及信道的容量应该为 1。观察图 3，可以得知，在给定初始标识 M=[1,0,1,0,0,0,1,0]的情况下：

对$\forall s \in S$有$\forall M \in R(M_0)$：$M(s) \leqslant 1$

所以图 1 中的 Petri 网是安全的，这就验证了接收和发送缓冲区及信道的容量为 1。

(2)Petri 网活性对协议无死锁的验证

由图 3 可以得知，该 Petri 网模型的每个变迁都是活的，即图 1 中的网是活的，这就说明 0-1 停止等待协议是不会出现死锁的。

(3)协议状态间可达关系的验证

图 3 是一个强连通图，所以$\forall M_i, M_j \in R(M_0)$：$M_i, M_j$是相互可达的。这就验证了协议各个状态间是可达的，即协议没有多余的、孤立的状态。

(4)协议动作序列的合法性

由图 1 可以看出，发送方从位置 P_1 到位置 P_2 再回到位置 P_1 时，变迁 t_{10}和变迁 t_{11}各发生一次，而且必须发生一次。利用图 3 可以验证，当网从状态 M_0=[1,0,1,0,0,0,1,0]，经状态[0,1,0,0,1,1,0,0]再回到 M_0 时，可以有多种变迁发生序列如：$t_{10}t_2t_{11}t_1$ 或 $t_{10}t_6t_3(t_5t_3)^*t_9t_2(t_7t_4)^*t_{11}t_1$ 等等，但每种变迁序列都要使 t_{10}和 t_{11}发生且仅发生一次。这就说明 0-1 停止等待协议保证了送交接收主机的帧没有遗漏的，也没有重复的。对于动作序列的验证还有很多种情况，不再一一赘述。

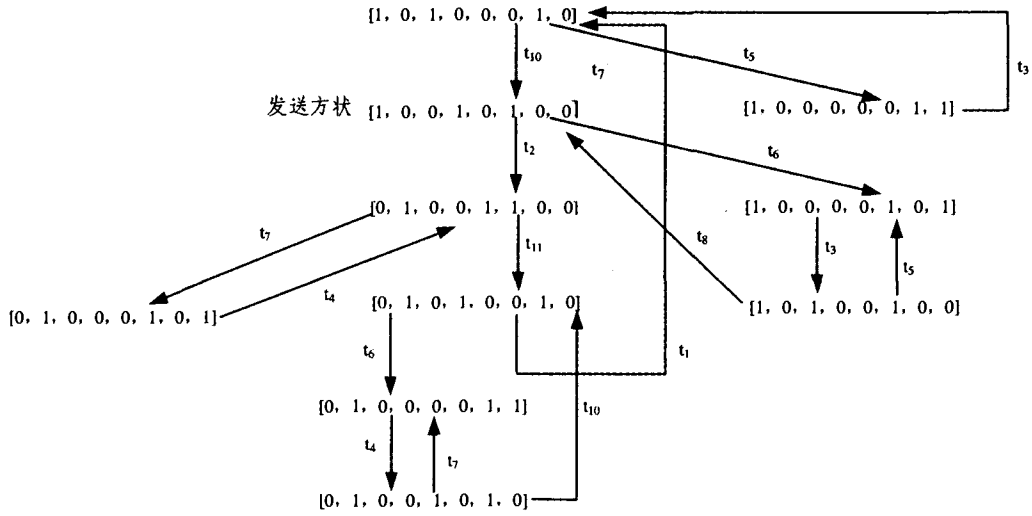

图 3　Petri 网模型的可达标识图

3.5　0-1 停止等待协议的性能评估

对 0-1 停止等待协议的性能评估本文采用时延 Petri 网，对图 1 网模型的各个变迁加上如下时延见表 3，所得的时延 Petri 网记为$\sum_2$。

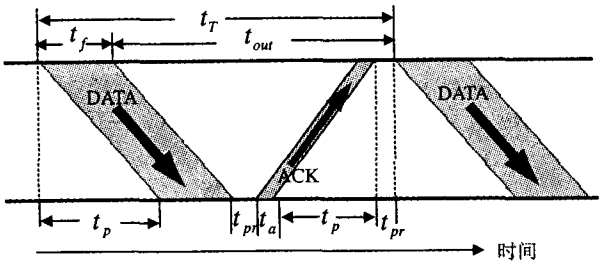

图 4　停止等待协议中数据帧和应答帧的时间关系

时延说明：

t_f：数据帧的发送时延。

t_a：应答信号 ACK 的发送时延。

t_p：数据帧或 ACK 沿链路传播的传播时延。

t_{pr}：收到数据帧或 ACK 后的处理时间。

t_{out}：超时定时器的设置时间。

变迁 t_1 的含义是收 ACK 发[0]帧，所以其时延定义为 $\tau_1=t_f+t_{pr}+t_p$ 即将 ACK 沿链路传播的传播时延也算作变迁 t_1 的时延。对于变迁 t_2、t_8、t_9、t_{10}、t_{11} 的时延也同理确定。t_5、t_6、t_7 的含义都是信号丢失，丢失过程可以看作是瞬时的，其时延为 0，但不是所有信号都要丢失所以定义其发生概率为 p。

对 0-1 停止等待协议作以下几点性能评估：

(1)超时定时器重发时间 t_{out} 的确定

超时定时器设置的重发时间应仔细选择。若重发时间选得太短，则在正常情况下也会在对方的应答信息回到发送方之前就过早重发数据。若重发时间选得太长，则往往要白白等掉很多时间。一般可将重发时间选为略大于“从发送完数据帧到收到应答帧所需要的平均时间”。根据图 3，“从发送完数据帧到收到应答帧”的动作序列为：

$M_0[t_{10}>M_1[t_2>M_2$

其中：$M_1=[1,0,0,1,0,1,0,0]$

$M_2=[0,1,0,0,1,1,0,0]$

$\tau_{10}=t_p+t_{pr}+t_a$　$\tau_2=t_f+t_{pr}+t_p$

根据动作序列 $M_0[t_{10}>M_1[t_2>M_2$ 可得到图 4。

由图 4 可知：

$t_{out}>t_p+t_{pr}+t_a+t_p+t_{pr}$

一般说处理时间 t_{pr} 和 ACK 帧的发送时间 t_a 都远小于传播时延 t_p，这样将重发时间取为略大于两倍的传播时延，为了讨论方便我们取为两倍的传播时延，即：$t_{out}=2t_p$。

(2)平均传播时延

由动作序列 $M_0[t_{10}>M_1[t_2>M_2$ 可知，两个发送成功的数据帧之间的最小时间间隔 t_r 为：

$t_T=\tau_{10}+\tau_2=t_p+t_{pr}+t_a+t_{pr}+t_p+t_f=t_f+t_{out}=t_f+2t_p$，由于 t_5，t_6，t_7 的发生概率为 p，此外，允许重发的次数不受限制，可以得出正确传送一个数据帧所需得平均时间 t_{AV} 为：

$$t_{AV}=t_T+(1-p)\sum_{i=1}^{\infty}ip^it_T=t_T/(1-p)$$

(3)最大吞吐量

每秒成功发送的最大数据帧数就是链路的最大吞吐量，记为 λ_{max}。显然 $\lambda_{max}=1/t_{AV}=(1-p)/t_T$

表3　Σ_2 的变迁延迟时间

变迁名称	时延	变迁名称	时延	变迁名称	时延
t_1	$\tau_1=t_f+t_{pr}+t_p$	t_5	$\tau_5=0$	t_9	$\tau_9=t_p+t_{pr}+t_a$
t_2	$\tau_2=t_f+t_{pr}+t_p$	t_6	$\tau_6=0$	t_{10}	$\tau_{10}=t_p+t_{pr}+t_a$
t_3	$\tau_3=t_{out}$	t_7	$\tau_7=0$	t_{11}	$\tau_{11}=t_p+t_{pr}+t_a$
t_4	$\tau_4=t_{out}$	t_8	$\tau_8=t_p+t_{pr}+t_a$		

总结　同已有的文献相比较，本文的特点是用原型 Petri 网构建协议的模型并对协议的正确性进行验证，然后在原型 Petri 网中加入时间因素转化为时延 Petri 网，用时延 Petri 网对协议进行性能评估。这样，在协议的正确性验证部分，可以最大限度利用 Petri 网理论中的已有成果，并且在不改变模型的基础上对协议做出严格的性能评估。文中通过实例给出了利用原型 Petri 网对协议验证的方法，对 0-1 停止等待协议进行了较完备的静态和动态的形式化验证，通过对原型 Petri 网的变迁赋予延迟时间，方便地把原型 Petri 网转化为了时延 Petri 网，并利用时延 Petri 网对协议进行了严格的性能分析，这也是本文的特色之一。我们将进一步研究利用 Petri 网的语言和语义对协议进行语义验证。

参 考 文 献

1　Avresky D R. Formal verification and testing of protocol[J]. Computer Communications, 1999,22:681～690

2　Qing SH. Design and logical analysis of security protocols[J]. Journal of software, 2003, 14(7): 1300～1309

3　Tarigan A. Survey in Formal Analysis of Security Properties of cryptographic Protocol[J]. IEEE, 2002.5

4　Shiu-Kai Chin Susan Older. Formal methods for assuring security protocols[J]. In the Computer Journal, volume British computer Society, 2002,45:46～54

5　罗军舟，等. Epr/TN 网可达性分析的冗余并发后继标识[J]. 计算机研究与发展，1998,35(3):251～254

6　Wang Junfeng , Yang Jianhua , Xie Gaogang , Zhou Mingtian . OSFPv3 Protocol Simulation with Colored Petri Nets[C]. In: Proc. of ICCT 2003

7　Kelling C, et al. Modeling priorities in token protocols with timed petri ets[J]. International Journal of Mini and Microcomputers, 1995, 17 (1) : 35～ 41

8　张广胜，吴哲辉，逄玉叶. 基于时间 Petri 网的密码协议分析[J]. 系统仿真学报，2003,15(增刊)

9　袁崇义. Petri 网原理[M]. 电子工业出版社，1998

10　Murata T. Petri nets: properties, analysis and applications[A]. Proc, IEEE, 1989, 77(4): 541～580