ISSN1000-9825 Journal of Software 软件学报 2000,11(5):606~615

从 Petri 网到形式描述技术和协议工程*

罗军舟 沈俊 顾冠群

(东南大学计算机科学与工程系 南京 210096)

E-mail: jluo@seu.edu.cn

摘要 协议是计算机网络的命脉,协议复杂性的提高导致了协议工程学科的出现.该文首先分析了协议工程各项活动的内容、方法和相互关系,讨论了各种形式描述技术(formal description technique,简称 FDT)的特性及其优缺点,从而引出基于 Petri 网理论的 FDT.该文说明了 Petri 网作为协议描述技术的优势,指出当前基于 Petri 网的协议工程研究的难点,其中面向协议开发的网工具是一项重要的研究内容.按照开放系统互连参考模型的层次,总结了国际上的研究进展情况,并阐述了未来的研究趋势.最后从协议描述、协议验证与分析以及辅助测试与实现这 3 个角度给出了基于 Petri 网的协议工程的基本方法.

关键词 协议,协议工程,形式描述技术,Petri 网.

中图法分类号 TP311

当前,人类伴随着信息革命正步入计算机网络化的信息时代,21 世纪全世界将成为一个网络大家庭.计算机网络的发展是网络协议设计和开发的结果,协议与网络同存亡共患难,协议是网络的血液和生命.在 20 年左右的网络发展史中,IBM SNA,ISO OSI/RM 和 DoD TCP/IP 等著名体系结构和协议已发挥了不可估量的作用,SNA 是协议体系结构的开拓者,OSI/RM 是协议的指路灯塔,TCP/IP 是目前盛行的事实上的工业标准[1].XTP,VMTP,Delta-t 和 NETBLT 的出现,将使计算机网络进入一个高速和高性能的时代.

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,协议再也不可能用工程直觉方法进行高质量的设计,协议的完整性、正确性、安全性、可移植性和标准化都难以得到保证,而且协议实现后纠正协议描述错误的代价是十分可观的.错误导致服务可靠性的降低,会引起用户极大的失望,在这种情况下,需要合适的方法、技术和计算机辅助工具来设计和维护网络协议.协议工程(protocol engineering)[2]用形式化的方法描述在协议严格的设计和维护中的各个活动,它是研究以对象为协议的软件工程的,但所建立的协议设计方法比现有软件工程的一般方法更严格,从而使协议开发整个过程一体化、系统化和形式化.

1 协议工程活动

协议工程覆盖协议生命期活动的整个范围[3~5],主要的设计和开发活动包括:

- 分布式计算资源的用户需求;
- 高级体系结构设计,通常建立某个协议集提供的服务分层结构;
- 分层结构中各层服务的描述;
- 分层结构中各层协议的描述,通常分为:(1) 符合国际标准的独立于实现的描述;(2) 考虑环境因素的逐

* 本文研究得到国家自然科学基金(No. 69873009)和国家 973 信息技术与高性能软件项目基金(No. G1998030405)资助.

作者罗军舟,1960 年生,博士,教授,主要研究领域为协议工程,Petri 网应用,网络安全,网络管理.沈俊,1975 年生,博士生,主要研究领域为协议工程,Petri 网应用,网络管理,多 Agent.顾冠群,1940 年生,教授,博士生导师,中国工程院院士,主要研究领域为协议工程,高性能网络,分布对象计算,Petri 网应用.

本文通讯联系人:罗军舟,南京 210096,东南大学计算机科学与工程系

本文 1999-06-10 收到原稿,1999-12-06 收到修改稿

步求精的实现描述;

·目标实现

协议的实现必须与协议的用户需求相一致,包括综合和分析两种方法.综合是向协议设计者提供一套从描述到实现用户需求的形式求精规范,保留所需特性,包括协议综合(protocol synthesis),即由相邻服务描述产生协议描述的规范;自动实现(automatic implementation),即协议描述到某个协议实现的转换.

在协议分层结构中,要检验详细描述与较抽象描述是否一致,用分析技术来证明所需特性已被保留,不需要的特征已被舍去,包括协议验证(protocol verification),即证明协议描述正好提供服务描述中所表示的需求,它与协议综合互补;一致性测试(conformance testing),即让协议设计者相信协议实现确与协议描述一致,它与自动实现互补.

协议工程活动还包括性能评价(performance evaluation)、维护(maintenance)和协议变换(protocol conversion).性能评价涉及到吞吐量、时延以及可靠性等实时性质,协议维护包括纠正实现中的错误、更新协议文本甚至提出全新协议,协议维护需要对以上系列协议工程活动作一致性的修改.协议转换运用于协议体系结构不兼容的通信系统之中,例如,SNA 网络与 DECnet 网络互连,需要两个体系结构相互转换.协议转换器的开发涉及服务定义、综合、描述、验证、性能分析、直接实现和测试等类似的问题.

协议设计和开发的主要活动及其相互间的关系,如图 1 所示.

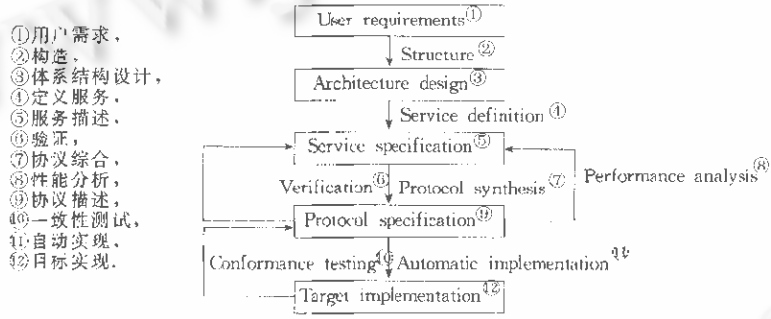

Fig. 1 Protocol engineering design activities

图1 协议工程设计活动

2 协议工程方法

图 1 同样也给出了以下协议设计的自顶向下方法:

·分布式用户应用需求分析,建立文档;

·协议分层的体系结构设计,满足所需求要求;

·定义协议分层结构中各层的服务,这需要分成两步来做:

(1) 整体描述,即抽象描述服务使用者和提供者的行为,定义服务原语序列集合和服务原语在使用者接口处的关系;

(2) 整体描述的逐步求精,即定义准确的且与实现无关的接口,将使用者和提供者的行为分离;

·描述分层结构的各层协议或协议类,包括在服务描述求精过程中为每个服务使用者定义一个协议机,在这个阶段应进行协议验证和性能评价;然后进一步求精建立实现描述,包括使用者和协议实体接口、目标实现限制与设计决策关系(什么软件、哪个操作系统、什么语言、如何并行操作、什么数据结构等问题)等详细描述;

·由实现描述产生目标实现的编码;

·一致性测试调试,严格测试协议的实现,是否符合协议描述要求以及错误是否被纠正.

3 形式描述技术

为了提供协议设计的坚实基础,使用数学方法不但能够提供无二义性的描述,而且能够对描述进行形式分

析和求精.协议形式化是指使用形式描述技术(formal description technique,简称 FDT)贯穿协议开发的各个阶段,起始于协议规范描述,从而使协议的研究开发可以独立于非形式的自然语言文本和最终实现代码,避免了协议验证测试的复杂性[6].

理想的FDT应能支持协议工程活动的各个环节,特别是协议综合、验证、自动实现和一致性测试.利用数学技术允许开发描述语言的编译器和由描述派生的自动测试序列,这将大大提高协议实现和维护的能力,降低提供和维持信息服务的代价.一个FDT具有如下一些重要特性:

- 完整的语法和语义定义;
- 体系结构、服务和协议的可表达性;
- 协议重要特性(如,无死锁)的可分析性;
- 支持复杂协议的管理(如,构造能力);
- 支持逐步求精的方法;
- 支持实现独立性(包括并发性、非确定性和适当的抽象机制);
- 支持协议生命期的各环节,包括验证、实现和测试;
- 支持自动设计、验证、实现和维护方法.

形式描述技术(FDT)有多种,主要包括状态变跃技术(如Petri网、有限状态机FSM等)、抽象数据类型、文法、时态逻辑(temporal logic)、高级程序设计语言、集合论和过程代数(process algebra)等,还有一些混合技术.大多数扩展的状态变跃技术具有坚实的数学基础.例如,Bell实验室开发的Selection/Resolution模型提出了一个形式框架,从数学上给出了精确的语义,为状态机的构造定义形式代数积,阐述了化简方法,解决了可达性分析时的状态爆炸问题,提供了逐步求精方法.但是这个模型是同步的,所有处理由同一个全局时钟控制,数据流没有表示,抽象级太低.一般来说,扩展的状态变跃技术缺乏形式语义,分析功能较弱.在所有具有并发功能的程序设计语言中,几乎没有哪种语言是支持非确定性的,而且大多数语言比较复杂,分析也较为困难,没有达到具备实现独立性的抽象程度.当然,程序设计语言的最显著的优点是只要有编译器,描述可以直接实现.过程代数很有发展前景,它具有一套完善的等价理论,如果与网论相结合,则可用一套完善的分析技术提供一个结构清晰的模型.大多数的抽象方法(时态逻辑、集合论等)描述严密、实现独立性完好,但几乎不能直观地描述性质,分析不很复杂的协议也十分困难,并且需要手工证明,目前还缺少这些技术的辅助工具.

目前主要有3种FDT的国际标准,分别由ISO和CCITT制定.第1种是在1976年由CCITT(ITU)颁布的SDL(specification and description language),这是一种基于扩展状态变跃图和抽象数据类型的混合技术,已被电信公司广泛用于描述电子分组交换系统.80年代,ISO在制订OSI参考模型时,发布了两个FDT,即Estelle(extended state transition model language)和LOTOS(language of temporal ordering specification),在1988年确立了最后的国际标准文本.Estelle也基于扩展的状态变换模型,但使用的是PASCAL语法和数据类型.80年代初有人曾试图协调Estelle和SDL,终因没有共同的语义模型而失败.Estelle和SDL有3个弱点:(1)语义需重新定义;(2)缺乏分析技术;(3)实现不具有独立性.LOTOS提供形式语义,保证描述不存在二义性,便于分析和一致性测试理论的研究.LOTOS有两个组成部分,一部分基于过程代数,另一部分是基于ACT ONE的抽象数据类型.

由于上述原因,人们于是希望有一种与被建模的物理系统极为相关的理想FDT.它应具有较好的可读性,尽可能地避免描述者人为的构造,设计和实现过程中各成员通信方便,适合于数学运算并易于分析.这种FDT将减轻建立现实系统模型的困难,成为一种"自然"的描述技术.

4 基于Petri网的FDT

Petri网理论是在并发的概念上建立起来的,它直观地表示了非确定性,可用于表达不同抽象级上的系统概念.Petri网能用许多方法构造,例如,用简单Channel/Agency网来表示系统结构,在逐步求精后定义系统的行为.高级Petri网提供划分系统特点的方法,用另一种方法表示系统结构.Petri网通常表示为一种物理系统极为相近的图形形式,使人们能够比较容易地学习和理解这种描述语言.

Petri 网有一套成熟的数学理论工具,建立了许多分析技术,包括可达性分析、不变量分析(使用线性代数方法)、保持特性的变换(包括化简)、构造理论、形式语言理论、同步距离以及网的分解和等价.网的形式基础使网与其他并发模型建立了连接,这对于分布式系统的描述和分析是很有益的.近几年来,人们的注意力集中在如何将代数的抽象数据类型融合在高级网结构中,极大地方便了表示描述协议和服务所用的高级 Petri 网系统.

FDT 是协议工程中最基本也最重要的研究课题,ISO 和 CCITT 都十分重视对它的开发.FDT 直接影响到协议工程的各项活动,对照 FDT 的要求,目前还没有出现一种十分令人满意的 FDT.选择 Petri 网为研究 FDT 的对象,有以下几条依据[7~10]:

(1) 3 种标准 FDT 只支持协议工程的 1~2 个活动.

• Estelle 是一种过程语言,可以描述协议细节,用它描述的协议仅便于实现;

• LOTOS 描述协议实体的外部行为,不关心实体内部变化,用它描述的协议抽象级别高.LOTOS 定义了一套证明行为表达式的形式系统,用它描述的协议仅便于验证;

• SDL 是一种混合式的 FDT,缺乏形式语义,缺乏分析技术.

(2) Petri 网具有异步特性并发,因而决定了它的主要应用方向是分布式系统.根据外延公理,一个变迁的发生完全由它的外延决定,而与系统全局状态无关.因而,网系统是异步并发的"自由王国",没有主宰全局的中央控制.这一点十分适合网络体系结构、协议和服务的特点.

(3) Petri 网具有直观的图形表示形式,与物理系统相近,学习和理解这种语言相对容易.

(4) Petri 网最大的优点是具备一套严密的数学理论,各种技术极有利于验证和分析.

(5) Petri 网表现出面向对象技术的各个特性,将是一种优良的可用图形表示的面向对象语言.

(6) Petri 网是协议工程中的研究热点和有国际倾向性的协议开发技术.有人推测,现有的协议形式描述技术必须具有一个公共语义模型,能够把这些技术转换成公共模型,并且分析、仿真和测试的各个工具都基于公共模型.Petri 网可能为 Estelle,LOTOS 和 SDL 这 3 种标准 FDT 提供如上所述的一个公共模型.

5 当前的研究难点

最早从事 Petri 网描述协议研究的是加利福尼亚州立大学 Irvine 分校的 Merlin 博士,1974 年他发表了"计算系统可恢复性的研究"的博士学位论文.法国的 Diaz 博士研究了基于 Petri 网的协议描述技术,提出了协议描述和验证的方法[8].Bertelot 和 Terrat 又作了具体的论述[11].德国 GMD 的 Burkhardt 等人在 PROSIT 计划中运用高级网系统,阐述了描述 OSI 服务和协议的方法学.在 80~90 年代,澳大利亚的 Billington 教授概述了网在协议工程中的应用[6,10,12],Diaz 详细研究了网在协议描述和验证中的方法[8,13].高级网系统已被用于许多复杂协议和服务的描述和分析之中.

然而,这些研究碰到了各种困难,成果都未能较好地得以应用.主要表现在 3 个方面:(1) 没有建立一个抽象程度高、语义表达能力强和与协议系统接近的高级 Petri 网模型.按照 Petri 网理论证明,这种形式技术应有足够的描述能力来满足网络协议的要求,合适的 Petri 网建模,有利于协议工程中各项活动的描述;(2) 不支持整个协议工程的生命周期,大多数研究只局限于协议描述和验证;(3) 没有有效地集成专用工具进行协议的设计和开发,虽然出现了许多计算机辅助工具,但是描述工具、验证器、编译器和一致性测试器等工具都是分别单独开发的,它们使用同一种网系统的各种变体作为形式描述技术.

具体来讲,当前国际上基于 Petri 网的协议工程研究难点主要表现在以下 4 个方面:

(1) 自然语言描述的协议系统到 Petri 网系统的转换,相应的计算机辅助工具的开发,中间语言、一般模型、转换算法和规则的建立;

(2) 协议 Petri 网描述到协议实现的自动化,建立 Petri 网编译系统,实现网系统到目标代码转换的算法和模型;

(3) Petri 网节点和可达状态的爆炸,包括适当的高级网系统和分层网系统建立、网系统的合成与化简以及协议工程工作站的建立;

(4) 所建立的 Petri 网模型支持协议描述、协议验证、协议实现、性能分析、一致性测试等协议工程的各项

活动.

6 协议开发网工具

利用计算机开发集成Petri网的网图编辑、验证、分析和仿真功能的工具软件是Petri网研究的一项重要内容.

各种Petri网(包括高级网)工具已开发多年.1985年,F.Feldbrugge列出了26种工具[14],经过修改和完善,后来他又给出了19种.一些重要的专用网工具包括,加州大学Irvine分校研制的P-Nut系统,西德GMD的Nessy工具,Helsinki技术大学数字系统实验室开发的PRENA分析器以及GMD的SEGRAS系统.由于Petri网具有直观的图形表示形式和较强的分析能力,大多数工具提供图形编辑器、仿真器和包括可达性、不变量、化简等性质在内的系列分析工具.PROTEAN系统由澳大利亚远程通信研究实验室开发,它已广泛应用于通信协议的验证之中.最近,丹麦Aarhus大学的Jensen教授领导开发的有色网通用设计工具Design/CPN比较成熟,具有很强的功能和友好的人机界面,正在全世界范围内免费赠送和大力推广,值得注意.国内也有多所大学开发出自己的Petri网协议分析器,如东南大学计算机科学与工程系研制了一种面向扩展谓词/变迁网的PESAT系统[15],它运行于OPEN WINDOWS平台,已经应用于多种协议的描述验证之中.

在开发系统性能分析的计算机辅助工具方面,人们已经做了大量的工作,大多使用各种形式的随机Petri网和时间Petri网.这个领域的研究发展较快,1985年便首次召开了两年一次的国际Petri网和性能模型研讨会.

编译器的研制并不为人们所重视.PROMPT系统提供一个高级Petri网到C语言的编译器,可以选择跟踪或运行错误检查,还提供一个功能很强的符号调试器.这个高级Petri网包括Abstract Syntax Notation One子集,保证对于各类通信协议的应用.PROMPT具有良好的可移植性,可在UNIX,VMS和MS-DOS下运行,已用来实现CCITT公用信道信号系统七号信令(CCSS NO.7).

然而,对已经出现的这些图文并茂产品来说,大多数仍基于某种特定的Petri模型,往往不具备建模通用性,不支持协议工程的各个阶段活动,具有完备分析能力的Petri网辅助工具还很少,高级Petri网的不变量自动分析也是难点.因此,随着计算机技术的发展,开发支持协议工程活动整个生命期的Petri网辅助工具任重而道远,极具挑战性.

7 国际研究成果

国际标准化组织ISO定义的开放系统互连参考模型OSI-RM是被人们广泛接受的计算机网络模型.目前,ISO制定和颁布的协议都以此模型为基础,它将网络分为7层,自底向上分别是物理层、数据链路层、网络层、运输层、会话层、表示层和应用层.层与层之间属于嵌套关系,第N层的功能机制称为(N)-实体.网络通信协议是计算机网络中相同层的两个或多个实体间相互通信时所必须遵守的语义规则和语法格式的集合.协议通过协议规范以某种语言的形式确切定义.OSI模型作为一种抽象的标准是协议工程研究的主要对象,基于OSI模型的协议工程方法具有普遍意义.

协议包含6种元素:服务原语和服务原语时序、协议数据单元(PDU)和PDU时序、协议状态、协议事件、协议变量和协议行动/谓词.它们涵盖了协议的外部特征、内部机制和运行环境.协议的主体是它的状态-事件转换机制.具体内容有连接维护、数据组织、传输控制、通道管理等.一个好的协议应该满足:(1) 活性,即从任何一个状态开始运行都能正确到达指定状态的特性,因此,协议总能回到初始状态反复运行,满足回归性;(2) 安全性,即协议运行时不能出现死锁或活锁、错误的状态/动作、不能接收的事件等情况;(3) 一致性,即协议的外部特性(服务)与内部机制(协议机)所表现的特性一致;(4) 完备性,即协议运行不能出现二义性事件或状态,同时符合环境的各种要求.

7.1 各层研究

Petri网及其各种扩展模型在协议工程中的应用比较广泛,本文拟按照ISO开放系统互连参考模型OSI的7层结构给出一些较为具体的例子.

在物理层,协议主要涉及数据信号传输的电气特性和控制,如握手-应答机制、时序关系等,具体表现为通信芯片的设计,其基础是通信协议要求的事件-动作集.Petri 网可以用于建模、模拟运行和冲突检测等.墨尔本大学的 Ho 及 Forward 等人应用一种层次化和模块化的硬件 Petri 网(H-PN)进行通信协议的描述和验证,并且开发了能自动生成硬件实现的设计环境;法赫德国王大学的研究者还应用 Petri 网辅助设计通信协议控制器所需的超大规模集成电路.

数据链路层协议向网络层提供以帧为基础的数据传送服务,按照不同的原则划分为面向连接和无连接协议、单链路和多链路协议、面向字符和面向二进制比特协议等.数据链路层协议的功能通过服务原语来体现,内部表现为通信双方的状态-转移规程,一般形式为状态转换图或转换矩阵(表).Petri 网模型可以方便地由状态转换图生成,但是在许多场合,一些特殊的语义很难用传统 Petri 网来描述,因此,研究者提出了许多扩展系统.如日本静冈大学的 Takashi Watanabe 在时间网和有色网的基础上集成 Horn 子句以描述差错处理和放弃操作,并且通过层次化的方法缩减了状态空间规模[16];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,以上两种方法都已应用于差错恢复协议的建模和验证[17,18];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[19].另外,国内的林闯应用随机 Petri 网,结合马尔可夫链模型分析了 ATM 协议的性能特征.

在系统控制机制上,网络层和数据链路层没有很大的区别,网络层主要增加了路由选择以及流量控制等功能,因此,对于协议规程的描述与数据链路层基本类似,依然是通过形式化状态转换图的途径来建立 Petri 网模型.但有些研究者为了适应描述路由的需要而引入新的语义,如康斯坦丁大学的 Bettaz 等人正应用结合 Petri 网和抽象数据类型的 ATNet(代数项网)来描述网络协议,路由表及其操作由特定的数据类型和运算来表征[20].

运输层协议向上层提供可靠的端-端数据传输服务.OSI 根据下层协议提供的服务和上层协议的服务要求将运输层分为 5 类.虽然协议基本机制仍与数据链路层相似,但由于技术的和历史的原因,运输层的协议研究非常复杂,是协议工程研究中课题最多的部分.在保证基本数据传输、可靠性、流量控制、多路复用以及连接建立和维护等主要功能以外,运输层的性能评价也是非常重要的问题,因此研究者对运输层协议的形式化描述投入了更多的关注.TCP 协议是对应于运输层的、广泛应用于 Internet 且比较成熟的传输控制协议,但是,由于网络技术和用户需求的发展,人们提出了许多新的协议以满足高性能网络及多点投递的要求,它们的验证和分析显得格外必要,Petri 网在这方面也发挥了突出作用.如法国的 Younes Souissi 等人应用模块化的 Petri 网描述验证方法发现了 XTP(eXpress transport protocol——一种新型的高性能网络协议)协议中的用模拟方法找不到的错误[21];韩国的 Lee Jong-kun 等人则在群通信领域的多点传输协议 MTP 方面应用了 Petri 网工具,同时研究了相应网模型的削减问题[22].

会话层及其以上层主要面向应用进程,统称为高层协议.建立在通信实体之上的高层协议的 Petri 网建模和验证有了新的特点和要求.最基本的仍然是网络通信实体间交换数据信息和控制信息的机制,即相应 Petri 网模型的框架与低层协议大同小异,但是,由于附加了许多高层应用的特定语义要求,Petri 网必须作相应的扩展.比如,在多媒体环境中,服务质量表现为接收媒体数据流量相对于数据缓冲器大小引起的颤抖,要求提供拥挤反馈控制和接入控制以及服务器和客户机之间的松耦合同步,美国 Rutgers 大学的 J. Y. Hui 等人将 Petri 网引入了这方面的研究[23];在网络数据加密领域,加拿大的 A. M. Basyouni 应用有色 Petri 网的数学矩阵工具研究加密算法的精确性[24];韩国的 Lee Gang-Soo 提出一种加密时间 Petri 网——CTPN 以及相应的分析方法,用于研究安全协议[25];东南大学提出的一种时间 Petri 网——同步扩展谓词/变迁网 SYNEPr/TN 系统不仅可以用于多媒体协议,同样适用于网络安全协议超时机制的描述,而且能消除引入禁止弧和删除弧带来的 Petri 网模型的不确定特性[26].另外,在 OSI 模型中涉及的每一种应用层协议,如 FTAM,MMS 等以及 CSCW,CIMS 等复杂环境都为 Petri 网提供了用武之地,它们的主要特征是基于模块化和层次化方法简化网模型,结合有色网和时间网提供更为复杂的抽象语义等.

7.2 研究趋势

由于传统的协议形式化方法已经形成标准,基于 Estelle 和 LOTOS 的协议描述以及基于 TTCN 的协议验

证技术已经比较成熟;而且经过长时间的努力,高级 Petri 网的标准化工作已经提上议事日程,为此,协议工程研究人员在形式化模型间的转换方面做了很多工作,使得模型互相补充成为可能.如澳大利亚的Jirachiefpattana开发出转换 Estelle 到数字 Petri 网的工具[27],并且用于网络协议描述模型的自动转换和验证,但是,NPN 不能描述 Estelle 的优先级,延迟子句的缺陷也没有解决.

随着网络底层技术的进步和高层应用要求的提高,特别是 ATM 和多媒体通信应用需求的出现,网络协议的研究进入新的阶段.如何有效利用网络资源满足应用需求成为协议工程研究者的热门话题.因此相继出现了许多高性能协议,它们的形式化描述提出更高的要求,如何构建适当的 Petri 网模型成为新的课题.法国的 M. Diaz利用对象组合 Petri 网模型 OCPN 和时间流 Petri 网模型 TStreamPN 构建了一种主动网络体系结构[13],它吸收集成层间处理 ILP 的思想,将应用的处理能力集成到网络机制中,应用能够灵活选择对应于 QoS 的服务.

8 协议工程 Petri 网方法

8.1 协议描述

一组通信实体可以描述为单一的或成组的相互通信的 Petri 网模型,网间通信由直接耦合或者由库所和变迁表示的通道实现.网络的动态特性如控制和数据流由发生规则和标记分布描述.下面给出最简单的协议 Petri 网模型,首先是单工协议,如图 2 所示,其中的虚线表示系统的输入和输出.图 3 可以看作是一个半双工模型.

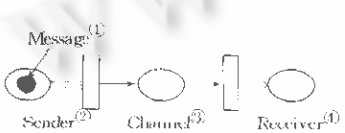

Fig. 2 Simplex protocol net graph
图2 单工协议网图

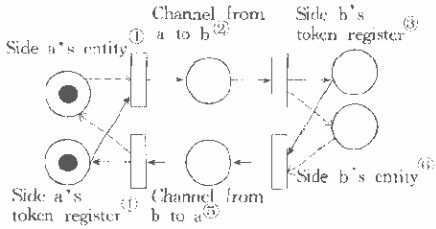

Fig. 3 Half-Duplex protocol net graph
图3 半双工协议网图

通信双方只有在有发送权时才能发送报文.对于全双工协议只需将图 3 中发送权寄存器库所及其联结的弧删去即可.以上几种模型都默认通道是可靠的,并且没有缓冲区.而实际的协议需要考虑通信双方及通道的许多功能特性,相应的 Petri 网模型要复杂得多.

为适应不同规范及验证的需求,从基本 Petri 网模型衍化出许多扩展模型系统,如谓词/动作 Petri 网、时间 Petri 网(TPN)、带时态逻辑的 Petri 网、有色 Petri 网(CPN)、面向对象 Petri 网(OOPN)、随机 Petri 网(SPN)以及数字 Petri 网(NPN)等.如多媒体网络协议最核心的问题是媒体流间的同步,引入时间限制的 Petri 网更适合建立形式化模型;在评价网络协议,特别是较低层协议的性能时,应用同构于连续时间马尔可夫链的随机网可以进行定量的稳态分析;面向对象 Petri 网由于能够映射软件工程的基本思想方法,如继承和类,则更多地应用于分布式系统的辅助设计.

8.2 协议验证和分析

对于单个特定协议的验证可能涉及专门的技术,而可达性分析和不变量分析是验证大多数协议的基本途径,Petri 网模型的许多性质都可以由它们推导出来,这为映射相应协议的性质提供了可能.而 Petri 网自身具备的可运行性方便了系统形式化描述级的模拟.

(1) 可达性分析是指生成 Petri 网的全部可达状态,以检查是否符合协议所要求出现的状态以及期望的行为特征,通常包括死锁、意外接受/发送、变迁活性以及库所标记数的有界性等.可达性分析从初始全局标识开始,根据每一个点火变迁或并发变迁集(同时具备点火条件的变迁的集合)生成分支结点,总体上形成可达图(reachability graph,简称 RG).

(2) 不变量分析是求 Petri 网在特定执行模式下不变量的特性.研究最广泛且理论上最完备的两种不变量

是 P-不变量和 T 不变量. P-不变量对应于 Petri 网中标记总数保持不变的库所子集,它反映协议的守恒性,如 Stop-Wait 协议中的发送方、信道和接收方的缓冲器中的报文总数恒为 1. T-不变量是指保持网标识不变的变迁序列,它反映协议运作的循环或重复特性.

(3) 状态爆炸问题. 由于状态空间随着模型增长呈指数型增长,人们一直试图压缩 RG 或 Petri 网的规模. 目前主要有保持特性变换和构造/分解理论这两种途径. 前者的具体方法是,在保持有界性、活性等 Petri 网模型特性的前提下,增加生成可达图时的限制条件或在可达性分析之前间接地改变网模型,如用单个库所或变迁代替一个特定子网,建立层次化的可达图或网模型以及基于等价关系削减结点数等. 后者的关键问题是如何确定构造和分解 Petri 网的规则,手段仍然是划分子网,分析网元素间的相关性以及建立层次模型等.

(4) 其他分析功能. 由于 Petri 网具备严格的矩阵运算理论支持,它还能推导出许多系统行为特征,如等价关系、进程等;而 Petri 网与其他几种形式化描述工具的内在联系使得它能起到模型间的桥梁作用,已经出现许多自动正向/反向翻译 Petri 网与 Estelle 或 LOTOS 等语言的工具. 这里要特别提到的是,因为数学基础是随机过程(排队论),所以 SPN 能够用于协议的性能评价,定量地求解系统的主要性能指标,如报文队列长度(库所标记数)、吞吐量和丢包率等.

8.3 辅助测试和实现

协议的一致性测试目的在于检测所实现的协议实体与协议规范的符合程度,包括静态和动态两种要求,其关键技术是生成测试序列,主要途径是基于有限自动机或数据流图的. Petri 网的作用是利用模型间的映射加快测试序列生成速度或者分析应用模型的测试覆盖率等. Petri 网同其他描述技术一样,可以制导协议优化设计和自动/半自动实现,而它的易扩展性还可以自然地体现自顶向下、逐步求精或面向对象的思想. 另外,Petri 网最新的应用还包括通信协议的自动转换,如根据 TCP/IP 协议和 SPX/IPX 协议的 Petri 网描述分析二者的等价性可以生成协议智能转换器.

9 结束语

Petri 网模型已经成为协议工程的强有力的工具,国内外研究潜力很大,其前景取决于两方面的因素:一是 Petri 网模型本身的语义能力的开发,二是协议工程建模要求的发展. 目前仍有许多相关技术有待于进一步地提炼、改进或者扩展. 例如,还有几种对研究协议特性十分有用的不变量,如同步不变量、排斥不变量等,在保持特性构造/分解时必须予以考虑;其次,模糊或非确定环境下的协议验证已经成为 Petri 网研究的一个难点. 另外,基于 Petri 网的协议软件复杂性计算也是值得深入研究的工作[7].

本文介绍了 Petri 网应用于协议工程中的一些基本情况,忽略了一些具体技术细节,但愿能起到抛砖引玉的作用. 我们认为,任何一种应用于协议工程的形式化描述工具都同时存在优越性和局限性. Petri 网能够反映协议元素的各种性质,便于形象地观察协议的运行状态,由于抽象层次更高,它比 Estelle、SDL 和 LOTOS 等其他形式化语言描述能力更强. 同时,严格的数学理论体系使其具有其他方法无法比拟的分析和验证能力. 由于 Petri 网较之其他方法在描述协议复杂语义和时序方面需要进行扩展,并且从图形模型到协议的具体实现之间的距离较大,但同时,又正因为得益于 Petri 网的良好的扩展特性,这些问题将能最终获得全面的解决. 当然,这也正是 Petri 网理论和计算机网络协议研究者有待于进一步开展的工作.

参考文献

1 Gu Guan-qun, Gong Jian. Computer Network. Nanjing: Jiangsu Science and Technology Press, 1989
(顾冠群,龚俭. 计算机网络. 南京:江苏科学技术出版社,1989)

2 Rudin H. Protocol engineering: a critical assessment. In: Aggarwal S ed. Protocol Specification, Testing and Verification (VIII). Amsterdam: North Holland, 1988. 3~16

3 Jonsson B *et al*. Protocol Specification, Testing, and Verification (XI). Amsterdam: North Holland, 1991

4 Linn R J *et al*. Protocol Specification, Testing, and Verification (XII). Amsterdam: North-Holland, 1992

5 Aggarwal S *et al*. Protocol Specification, Testing, and Verification (VIII). Amsterdam: North Holland, 1988

6 Wheeler G R, Batten T J, Billington J *et al*. A methodology for protocol engineering. In: New Communication Services:

A Challenge to Computer Technology. Amsterdam: North-Holland, 1986. 525～530
7 Cheung To yat. Petri nets for protocol engineering. Computer Communications, 1996,19:1250～1257
8 Diaz M. Petri net based models in the specification and verification of protocols. In: Brauer W ed. Petri Nets: Applications and Relationships to other Models of Concurrency. LNCS 255, Berlin: Springer-Verlag, 1988. 135～170
9 Brauer W *et al*. Petri nets: applications and relationships to other models of concurrency. LNCS 255, Berlin: Springer-Verlag, 1988
10 Billington J. Protocol engineering and nets. In: Proceedings of the 8th European Workshop on Application and Theory of Petri Nets. Zaragoza, 1987. 137～156
11 Berthelot G, Terrat R. Petri nets theory for the connection of protocols. IEEE Transactions on Communications, 1982,30(12):2497～2505
12 Billington J. Specification of the transport service using numerical Petri nets. In: Sunshine C ed. Protocol Specification, Testing, and Verification. Amsterdam: North-Holland, 1982. 77～100
13 Diaz M *et al*. From multimedia models to multimedia transport protocols. Computer Networks and ISDN Systems, 1997, 29:745～758
14 Feldbrugge F, Jensen K. Petri net tool overview 1986. In: Brauer W ed. Petri Nets: Applications and Relationships to other Models of Concurrency. LNCS 255, Berlin: Springer-Verlag, 1988. 20～61
15 Luo Jun-zhou, Gu Guan-qun, Xie Jun-qing. Petri net based protocol analyzer. Chinese Journal of Computers, 1997,20(3):206～212
(罗军舟,顾冠群,谢俊清.Petri 网协议分析器.计算机学报,1997,20(3):206～212)
16 Watanabe T. Protocol verification tool with extended Petri nets and horn cluse. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1995,E78 A(11):1458～1467
17 Gu Guan-qun, Luo Jun-zhou. EPr/TN net system and the formal description technique of network protocols. Chinese Journal of Computers, 1994,17(supplement):93～96
(顾冠群,罗军舟.EPr/TN 网系统及网络协议形式描述技术.计算机学报,1994,17(增刊):93～96)
18 Shen Jun, Luo Jun-zhou, Gu Guan-qun. Redundant concurrentable successor markings in reachability analysis of EPr/TN net. Computer Research and Development, 1988,35(3):251～254
(沈俊,罗军舟,顾冠群.EPr/TN 网可达性分析的冗余并发后继标识.计算机研究与发展,1998,35(3):251～254)
19 Kelling C *et al*. Modeling priorities in token protocols with timed petri nets. International Journal of Mini and Microcomputers, 1995,17(1):35～41
20 Bettaz M *et al*. On reusing ATNet modules in protocol specification. Journal of System and Software, 1994,27(2):119～128
21 Souissi Y. Towards a modular specification and verification of protocols within layered architecture. IFIP Transactions on C: Communication System, 1994,C-22:35～50
22 Lee Jong kun, Lee Kwuang-hui. Modeling of the multicast transport protocols using petri nets. In: Proceedings of IEEE Singapore International Conference on Network/International Conference on Information Engineering. '1995. 106～110
23 Hui J Y *et al*. Client-Server synchronization and buffering for variable rate multimedia retrievals. IEEE Journal on Selected Areas in Communications, 1996,14(1):226～237
24 Basyouni A M. New approach to cryptographic protocol analysis using colored Petri nets. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering. 1997. 25～28
25 Lee Gang-Soo *et Al*. Petri net based models for specification and analysis of cryptographic protocols. Journal of Systems and Software, 1997,37(2):141～159
26 Luo Jun zhou, Shen Jun, Gu Guan qun. Synchro-Net system: a Petri net model for high-layer protocols. Journal of Software, 1997,8(supplement):202～210
(罗军舟,沈俊,顾冠群.适合于网络高层协议描述的同步 EPr/TN 网.软件学报,1997,8(增刊):202～210)
27 Jirachiefpattana A. Estelle-NPN based system for protocol verification. In: COMPASS-Proceedings of the Annual Conference on Computer Assurance. 1995. 25～29

From Petri Nets to Formal Description Techniques and Protocol Engineering

LUO Jun-zhou SHEN Jun GU Guan-qun

(Department of Computer Science and Engineering Southeast University Nanjing 210096)

Abstract Protocol is the lifeline of computer network. The rapid increasing of protocol complexity results in

a discipline of protocol engineering. Based on an analysis of the contents and methods of protocol engineering activities and their interrelations, first discusses main formal description techniques (FDTs) and their characteristics, compares corresponding strongpoints and weaknesses, and then leads to Petri nets based FDT. Secondly, the paper points out special advantages of the Petri nets based formal techniques and the current research difficulties in Petri nets based protocol engineering, among which protocol development oriented net tools are now very important research tasks. Thirdly, the paper summarizes international research advances in terms of OSI/RM layers and expounds research trends in this area. Finally, the authors give fundamental methodologies for Petri nets based protocol engineering in protocol specification, verification and analysis, and computer-aided testing and implementation.

Key words Protocol, protocol engineering, formal description technique, Pe