安全协议形式化分析与验证

肖美华 著

科学出版社

安全协议形式化分析与验证

肖美华 著

华东交通大学教材(专著)基金资助项目

科学出版社
北京

内 容 简 介

本书是作者多年从事安全协议形式化分析与验证相关科研工作的总结，主要对两种形式化方法做了归纳：基于 SPIN 工具的模型检测和事件逻辑。

全书主要内容如下：介绍了安全协议形式化分析的研究现状、主要技术流派，以及协议描述语言 ProDL，阐述了基于算法知识逻辑的网络安全协议模型检测分析方法，用于显式地刻画入侵者模型能力；在网络安全协议验证模型生成系统中，采用偏序归约、语法重定序以及静态分析等优化策略，有效缓解模型检测过程中状态爆炸问题；对事件逻辑进行扩展，提出一系列规则，对安全协议进行形式化描述，无需显性刻画入侵者模型，只需分析协议动作之间的匹配顺序关系即可对协议的安全性进行证明。

本书可作为高等院校计算机、软件工程、信息安全等专业高年级本科生和研究生的教材，也可供相关专业领域的科研人员参考。

图书在版编目(CIP)数据

安全协议形式化分析与验证/肖美华著. —北京：科学出版社，2019.11

ISBN 978-7-03-062633-2

Ⅰ. ①安… Ⅱ. ①肖… Ⅲ. ①计算机网络-安全技术-通信协议 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 228902 号

责任编辑：王 哲 / 责任校对：王萌萌
责任印制：吴兆东 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销
*

2019 年 11 月第 一 版 开本：720×1000 1/16
2019 年 11 月第一次印刷 印张：10 3/4

字数：210 000

定价：78.00 元

(如有印装质量问题，我社负责调换)

前　言

随着软件在尖端领域（铁路信号、核电站、航空航天、国家安全和网络通信等）的广泛应用，软件可靠性成为一个非常重要的问题。形式化方法的意义在于它能帮助发现其他方法不容易发现的系统描述的不一致、不明确或不完整，有助于增加软件开发人员对系统的理解，因此形式化方法是提高软件系统，特别是安全攸关（Safety-Critical）系统的安全性与可靠性的重要手段。

形式化方法在软件验证中的应用大致开始于串行程序验证，随后运用于反应式系统、并发系统、实时系统中，形式化方法采用数学与逻辑的方法描述和验证软件。从描述上讲，一方面是系统或程序的描述，另一方面是性质的描述。从验证来讲，主要有两类方法，一类是以逻辑推理为基础，另一类则以是穷尽搜索为基础的模型检测。

网络已经成为人类彼此沟通，获取信息，以及社会生产和生活活动的一种重要载体和手段。正确而安全的网络通信依靠安全协议来保证。所谓安全协议，是在通信协议中应用密码学的手段隐藏或获取信息，达到认证以及消息正确发送的目的。大部分的安全协议运行在复杂的分布式网络环境中，分布式网络具有多主体参与、大规模并发和运行动态性等特点，因此设计出的安全协议难免会存在安全漏洞。实践证明，许多安全协议在使用多年后被发现存在很严重的安全漏洞，例如著名的 Needham-Schroeder 公开密钥协议、Kerberos 协议和 SSL 协议的早期版本等（Needham-Schroeder 公开密钥协议在公开 17 年后，其存在的入侵者攻击漏洞才被 Lowe 发现）。因而，网络安全协议的研究具有很强的现实应用背景。

认证协议的设计与分析是十分复杂的。大量的实例说明，即使参加认证协议的主体只有 2 个或 3 个，在整个协议中交换的消息只有 3 条或 5 条，设计一个正确且没有安全缺陷的认证协议也是一项很困难的任务。因此，迫切需要一种合适的形式化分析方法，对认证协议进行严谨的形式化分析，检查认证协议是否达到其设计目标，认证协议是否存在安全缺陷或冗余等。

本书基于 SPIN 工具的模型检测和事件逻辑这两种形式化方法，对网络协议安全性进行分析。全书共分 7 章。第 1 章是绪论，介绍安全协议形式化分析背景及研究现状。第 2 章介绍形式化方法基本理论，包括：形式化方法概述、模态逻辑、模型检测、定理证明以及二者的比较。第 3 章讨论安全协议，包括：安全协议概念、分类；协议安全属性；协议安全构建方法；协议攻击者模型及其攻击类型。第 4

章研究采用模型检测技术，对网络安全协议进行形式化分析与验证，主要内容有：安全协议形式化表示，包括消息、动作、迹、消息状态及修改、消息生成规则等；阐述基于算法知识逻辑的安全协议形式化分析流程以及验证模型优化策略，并与其他形式化方法进行比较。第 5 章设计网络安全协议验证模型生成系统，包括：系统概述；系统设计与实现；设计协议描述语言 ProDL；Needham-Schroeder 公开密钥协议、BAN-Yahalom 三方对称密钥认证协议、CMP1 可信第三方电子商务协议分析与验证。第 6 章分析事件逻辑理论，包括：事件系统；事件逻辑公理、推论及性质；事件逻辑形式化描述协议；基于事件逻辑的安全协议证明；与其他典型证明方法对比。第 7 章是总结与展望，包括：研究成果总结、下一步研究工作。

本书是作者从 2002 年在中国科学院软件研究所攻读博士学位起，十几年来科研成果的系统总结，同时还参考了国内外的最新理论和技术进展。本书的研究得到国家自然科学基金(61163005、61562026、61962020)、中国博士后科学基金(20110491497)、江西省主要学科学术与技术带头人资助计划项目(20172BCB22015)的资助，同时还得到计算机软件新技术国家重点实验室开放课题、江西省自然科学基金（含重点）、江西省高校科技落地计划项目、江西省科技攻关计划（含重点）、江西省科技对外合作计划项目、江西省软科学科技项目、江西省教育厅科技计划等资助。

本书付梓之际，首先感谢作者的博士生导师薛锦云教授。同时，作者在从事形式化方法科研之路上，得到很多专家的帮助、支持与鼓励，他们是：林惠民院士、周巢尘院士、韩文报教授、张健研究员、张文辉研究员、曹珍富教授、林东岱研究员、沈一栋研究员、邵维忠教授、段振华教授、应时教授、孙晓明研究员、王戟教授、詹乃军研究员、董威教授等。作者于 2008 年 9 月～2009 年 9 月在美国做访问学者，感谢康奈尔大学 Constable 教授的邀请，他是形式化方法领域国际知名专家，访学期间与 Constable 教授、Bickford 博士合作，致力于运用事件逻辑理论对安全协议进行形式化分析。没有他们的教诲和指导，就没有本书的面世。

感谢研究团队中，多年来从事形式化领域研究并做出重要科研成果的博士生、硕士生，他们是：杨科、钟小妹、宋佳雯、李伟、李娅楠、程道雷、梅映天、谌佳、王西忠、马成林、李静、吴昌、刘欣倩、万子龙、余立全、谭杰、朱科、邓春艳、王兵、朱宜炳、熊昊、刘俏威、舒良春、胡磊、程莹、倪烨、尹传文、刘婷婷、胡凡玮、程进、刘惠萱、张坚林等。特别感谢本书出版、文字排版编辑工作团队成员的辛勤付出，他们是：宋子繁、周浩洋、李泽寰、张彤、欧阳日、易寒萧等。科学出版社给予了大力支持，王哲编辑为本书付出了辛勤努力，谨表谢意。同时，本书的出版还得到了华东交通大学教材（专著）基金资助，在此一并致谢。

本领域涉及的理论技术复杂，加之作者水平有限，书中难免存在不足之处，恳请读者批评指正，并将意见和建议发至：xiaomh@ecjtu.edu.cn，作者不胜感激。

肖美华

于华东交通大学孔目湖

2019 年 10 月

目　录

第1章 绪 论

1.1 安全协议形式化分析背景

随着互联网热潮向社会的每一个角落逐渐渗透，通过网络来获取信息、存储信息和交换信息的方式已经在人们生活中得到普及，大多数活动如购物、聊天、转账、学习等都是通过计算机在线完成，网络使得用户足不出户就能与世界互联互通，但是任何事情都有双面性，当前互联网虚拟空间与现实空间的危险叠加后，更容易给财产安全、社会稳定和国家安全带来严重影响。网络的强大能力在为人们生活带来便利的同时，也使网络成为竞争者之间相互角逐的战场。在这个战场中，信息窃取、数据篡改和网络攻击将成为影响力最大和杀伤力最强的武器。这不仅影响个人的日常生活，而且严重影响国家的政治、经济、军事安全。

开放性的网络环境导致用户无法判断其主动或被动接收的数据是恶意还是善意的，这使得人们在上网时会面临各种风险。例如，使用的社交账号被盗、电话号码和住址被公开以及私人照片被泄露等问题，严重的甚至会导致用户遭受巨大经济损失。开放性的网络环境使得互联网变得脆弱，这是因为对非专业人员来说，数据在网络中的传输过程是不可控且不可视的。

软件形式化方法，最早可追溯到20世纪50年代后期对于程序设计语言编译技术的研究，即Backus[1]提出巴克斯范式(Backus Normal Formula，BNF)作为描述程序设计语言语法的元语言，使得编译系统的开发从“手工艺制作方式”发展成具有牢固理论基础的系统方法。20世纪60年代，Floyd[2]提出的不变式断言和Hoare[3]提出的公理化方法都是用数学方法来证明程序的正确性。然而20世纪60年代以前，计算机刚刚投入实际使用，软件开发往往只是在计算机上设计和编制一个满足特定需求的应用，早期软件规模比较小，文档资料通常也不存在，软件可靠性和安全性问题不明显。到60年代中期，大容量且高速度计算机的出现，使计算机的应用范围迅速扩大，软件开发数量急剧增长，软件系统的规模越来越大，复杂程度越来越高，软件可靠性问题也越来越突出。1968年计算机科学家召开国际会议，第一次讨论软件危机问题。针对当时所谓“软件危机”，人们提出了各种解决方法，归纳起来有两类：一是采用工程方法来组织和管理软件的

开发过程；二是深入探讨程序和程序开发过程的规律，建立严密的理论，用来指导软件开发实践，该方法推动了形式化方法的深入研究，带来了形式化方法的研究高潮。

随着互联网的发展，由软件引起的安全问题涉及面越来越广，影响层次也越来越深，越来越多的安全协议也随之不断地涌现。但任何的网络都不是铜墙铁壁和无缝可循，即使网络协议设计之初堪称完美，时间一长协议漏洞也会暴露出来。例如，1978 年 Needham 和 Schroeder 提出著名的 Needham-Schroeder[4]协议，一直被认为是安全的。但是三年后，文献[5]指出，该协议并不能保证 PK(B)是当前 B 的公钥，也许是一个旧的密钥和已经泄露密钥的重演。所以，尽管安全协议在保障信息安全中起到了一定作用，但要判断一个协议是否能够在不安全的环境下正确地达到预定的安全属性却并不容易。因此，对协议进行安全性分析，找出协议漏洞，并改进相应的协议成为日益迫切的问题。

1981 年 Clarke[6]提出自动化验证技术——模型检测方法，主要通过显式状态搜索或隐式不动点计算来验证有穷状态并发系统的模态/命题性质，并能在系统不满足性质时提供反例路径。80 年代，Dolev 等开发了一系列的多项式时间算法用于对一些协议的安全性进行分析。Dolev 和 Yao[7]还提出多个协议并行执行环境的形式化模型，模型中包括一个可获取、修改和删除信息并可控制系统合法用户的入侵者，成功地找到了协议中未被人工分析发现的漏洞。1989 年 Burrows 等[8]提出 BAN 逻辑引起了人们广泛的关注。BAN 逻辑的规则十分简洁、直观，易于使用。BAN 逻辑成功地对 Needham-Schroeder、Kerberos 等几个著名的协议进行了分析，并找到了其中已知的和未知的漏洞。BAN 逻辑的成功激发了研究者们对安全协议形式化分析的兴趣，许多安全协议形式化分析方法在此影响下接连产生。1996 年 Brackin[9]推广了 GNY 逻辑并给出了该逻辑的高阶逻辑(Higher Order Logic，HOL)理论，之后利用 HOL 理论自动证明在该系统内与安全相关的命题，并首次把递归神经网络运用到定理证明问题上。2000 年 Denker 和 Millen[10]开发的 CAPSL(Common Authentication Protocol Specification Language)为协议形式化分析工具提供通用说明语言，标志着不同形式化分析技术的日趋成熟。

经过几十年的研究和应用，研究者们在安全协议的形式化分析方法这一领域取得了大量的和重要的研究成果。形式化方法已经从早期最简单的一阶谓词演算方法，演变成到现在基于逻辑、状态机、网络、进程代数和代数等应用于不同领域及不同阶段的方法。

1.2 安全协议形式化分析研究现状

安全协议形式化分析技术已有40多年的历史，并日趋成熟。随着网络的发展，安全协议面临着新的威胁，电子商务、多方通信、匿名通信和拒绝服务等问题的出现对安全协议设计与分析提出了更高的要求。随着网络环境愈加开放、攻击者能力不断增强和新型协议不断增多，形式化分析方法也在不断地发展。

近几年，国内外学者在模态逻辑方法基础上，主要针对模态语言、逻辑语法与语义、逻辑关系表达能力和方法应用范围等方面做了许多扩展性和创新性的研究。

例如，申宇铭等[11]刻画了命题模态逻辑表达能力——van Benthem刻画定理，给出描述逻辑ELU(含构造子：原子概念、顶概念、概念交、概念并和完全存在约束)的模拟关系，建立了ELU中概念和术语公理集的表达能力刻画定理。黄振华[12]引入结构化标记转换系统，提出结构化部分互模拟和结构化共变-逆变模拟，分别采用模态逻辑语言BL和CCL刻画逻辑关系。刘海等[13]在CEGS中引入效用函数和偏好关系知识，得到新的rCEGS，并在合作模态算子 Γ 中加入行为ACT参数，提出新的可形式化分析安全协议的交替时序认知逻辑rATEL-A，然后运用rATEL-A构建两方安全协议的形式化模型，并基于rCEGS的等价扩展式博弈，对具体的两方交换协议进行形式化分析。邓少波等[14]提出具有模态词$\Box\varphi=\Box 1\varphi\vee\Box 2\varphi$的命题模态逻辑，给出了该逻辑的语言、语法与语义，并将该完备的公理化系统记为 ${}^{S51}V^{S52}$。马明辉等[15]对关系语义(Kripke语义)下极小非正规模态逻辑C2进行时序化处理，得到极小非正规时序逻辑C2t，建立了具备可靠性和完全性的C2t的Hilbert式公理系统HC2t和加标矢列式演算系统GC2t。冉婕等[16]提出了增加交互操作符的UML顺序图的六元组形式化方法，对描述逻辑进行时序扩展，得到可表示动态和时序语义的形式化规范——时序描述逻辑，并用时序描述逻辑的时态算子得到时序描述逻辑语义形式的UML顺序图，用UML顺序图描述完整的C语言执行过程，将其形式化描述。Zadeh和Lotfi[17]构造了一个具有有限状态系统结构的模态逻辑模型(FS模型)。Larsen和Mardare[18]为能够表达WTS(Weighted Transition System)的定性和定量特性的多模态逻辑——加权模态逻辑(Weighted Modal Logic，WML)开发了证明系统，并提出WML对WTS的弱完备公理和强完备公理。Takács和Vályi[19]扩展了Coffey-Saidha-Newe模态逻辑以处理多信道协议，并使用扩展逻辑验证了MANA族中协议的有效性。Libal和Volpe[20]通过使用从模态语言转换为一阶极化语言和其小内核基于经典聚焦序列演算的检查器，描述了用类Prolog语言实现逻辑K的一般方法，并说明了如何将该方法扩展到其他模态

逻辑。Belardinelli 和 van der Hoek[21]研究了形式模态语言在人工智能领域的作用，介绍了二阶命题模态逻辑(Second-Order Propositional Modal Logic，SOPML)的多模态版本，阐明了其作为知识表示和时空推理规范语言的有效性。Hulst 等[22]提出一种非确定性自动机受控系统综合的新方法，限制不受控系统的行为规范，使其满足给定的逻辑表达式，同时遵守监督控制最大允许性和可控性的规则，将 Hennessy-Milner 逻辑从 Gdel-Lb 逻辑扩展为具有不变和可达模式的 Hennessy-Milner 逻辑。

近几年，国内外在形式化建模方面的研究有较为快速的发展。其中，形式化建模在特定领域的研究逐渐形成特色，不再局限于各种形式模型的研究，在程序分析、模型检测和混成系统等方面也做了许多工作。在软件形式化验证的理论、方法和技术等方面产生了大量有影响力的成果，形成了许多高效的软件形式化验证工具。但是模型检测的研究工作也不仅仅局限于协议安全性分析这一面，目前国内外已经有采用模型检测对人工智能算法等多方面进行分析、验证的工作。

例如，Fu[23]研究了理论的操作语义和观察语义，为异步理论构造了一个完整的公理系统，给出了异步π的弱异步双相似性的证明系统。陈双双等[24]从研究 CAD/CAE 模型转换出发，基于 VC 平台对 Pro/E 二次开发技术，实现了模型转换前 CAD 模型的预先检查。阚双龙等[25]提出使用事件自动机对 C 程序的安全属性进行规约，并给出了基于有界模型检测的形式化验证方法。赵岭忠等[26]提出了一种新的 CSP(Communication Sequence Process)指称语义模型——关键迹模型(Critical-Trace Model)及基于该指称语义模型的 CSP 模型检测方法，并开发了一个可同时验证多条性质、在性质不满足时还可提供多条反例的 CSP 模型检测原型系统——TASP。朱维军等[27]使线性时序逻辑模型检测技术不仅仅只在电子计算的平台上实现，为了以脱氧核糖核酸(Deoxyribonucleic Acid，DNA)为载体对线性时序(时态)逻辑(Linear Temporal Logic，LTL)实施模型检测，提出了一个可对 LTL 逻辑时序算子检测的新方法。葛徐骏等[28]对传统基于模型的测试方法的一致性检验进行了扩展，提出了一致性检验框架 ProMiner，可支持软件模型和代码间双向的一致性检验。梁常建和李永明[29]在模糊时态方面对 GPoLTL(Generalized Possibilistic Linear Temporal Logic)进行扩展，并定义其为具有模糊时态的广义可能性线性时序逻辑 GPoFLTL(Generalized Possibilistic Fuzzy Linear Temporal Logic)。张业迪和宋富[30]基于交替时态逻辑(Alternating Temporal Logic，ATL)提出了一种在语法层对智能体策略类型进行刻画的系统模型——带类型解释系统，引入策略类型属性，允许不同智能体具备不同的策略类型。国防科技大学的李运筹等[31]研发了并行程序验证工具 VASR-CBMC，该工具能够缩短验证时间，有效提升模型检验对并发程序的验证能力。Navabpour 等[32]提出以检查中的 C 程序和

一组 LTL 属性作为输入，并生成一个仪表化的 C 程序，程序在运行时被时间触发的监视器验证 RITHM(Runtime Time-Triggered Heterogeneous Monitoring)。Barnat 等[33]提出了一个并行分布式 LTL 模型检查器 DiVinE 的新版本，可用模型检查器验证系统类的扩展，支持并行和分布式内存处理，支持多线程 C/C++程序的直接模型检查和定时自动机的完全非定时 LTL 模型检查，以及与任意系统建模工具接口的通用框架。Din 等[34]开发了可用于基于 ABS 编写的并发和分布式程序进行验证的工具 KeY-ABS。Lomuscio 等[35]提出了一种用于多智能体系统验证的模型检验器 MCMAS。模型检验工具 MCMAS 可以支持有效的符号技术，用于根据表示时间、认知和战略属性的规范验证多 Agent 系统。Ngo 和 Legay[36]提出了如何使用统计模型检测直接对大型 SystemC 模型进行分析的方法。

近几年，国内外关于交互式定理证明在系统验证等方向的应用研究也明显增多，取得了一些显著的成果。研究者们不仅仅局限于定理证明方法的扩展和创新，更将方法应用到了生物和医疗等不同的研究领域中。

石刚等[37]开展了从同步数据流语言(Lustre 为原型)到串行命令式语言(C 为原型)的可信编译器构造的关键技术研究。韩世宁[38]提出一种基于协议组合逻辑(Protocol Composition Logic，PCL)的匿名性分析方法，通过将观察等价思想和 PCL 理论相结合，提出分析协议匿名性的形式化方法，通过实例分析说明了该方法的可行性和正确性。詹业兵[39]设计并实现了基于相继式演算的一阶逻辑定理证明器 FolProver，FolProver 可用于证明一阶逻辑中定理的正确性，具有图形界面，支持交互式证明和自动化证明，并具备保存和加载证明等多个便于使用的功能。张恒若和付明[40]在定理证明工具 Coq 中实现了一个自动证明策略 smt4coq，通过在 Coq 中调用约束求解器 Z3，自动证明 32 位机器整数相关的数学命题，提高了自动化验证的程度，减少了用户手动验证程序的开销。宋丽华等[41]在交互式定理证明器 Isabelle/HOL 中对 Miller 和 Myers 在 1985 年提出的基于行的文件比较算法 fcomp 进行了形式化，改正了算法关于边界变量迭代的一个小错误，证明了改正后算法的可终止性和正确性，对算法时间复杂性做了形式化分析，印证了算法的非形式化分析结论。钱振江等[42]在 Isabelle/HOL 定理证明器环境中对建立的内存管理模型和系统行为的操作语义进行形式化描述，并对内存管理模块的设计和实现的正确性进行验证。King 等[43]使用 SMT 求解器 CVC4 和 LP 求解器 GLPK 实现一种集成 LP 求解器的技术，在不影响正确性的前提下提高了 SMT 求解器的性能。Li 等[44]给出了 Isabelle 中一阶单变量多项式问题的一个完整的基于证书的决策过程，除了 Isabelle 的内核和代码生成之外，该过程依赖于不受信任的代码。Zhang 等[45]提出了一种基于 SMT 的 CCSL 形式化分析方法，该方法可证明 CCSL 约束的无效性。Rashid 和 Hasan[46]提出了一种基于演绎推理的

形式化方法——高阶逻辑定理证明，用于机器人细胞注射系统动力学行为的建模和分析。

如今，形式化方法越来越受到国内外计算机学术界的重视，欧洲设有专门的形式化方法组织(Formal Method Europe，FME)；美国计算机学会(Association for Computing Machinery，ACM)在2014年成立了SIGLOG(Special Interest Group on Logic and Computation)，涵盖计算逻辑、自动机理论、形式语义和程序验证等方向；中国计算机学会在2015年成立了形式化方法专业组，2018年成立了形式化方法专业委员会。形式化方法还成功应用于各种硬件设计，特别是芯片设计。IBM、Intel和AMD等各大硬件制造商都设有专门的形式化方法团队为保障系统的可靠性提供技术支持。由于形式化方法能够有效保证计算机软硬件系统的正确性和可靠性，因此许多国际标准化组织也将形式化方法列为保证安全攸关(Safety-Critical)系统必备的技术手段。形式化方法受到国内外行业越来越多的重视，使得用形式化方法验证软硬件产品的安全性和可靠性逐渐成为各行各业的首要选择。

参 考 文 献

[1] Backus J W, Bauer F L, Green J, et al. Report on the algorithmic language ALGOL 60. Numerische Mathematik, 1963, 6(1): 106-136.

[2] Floyd R W. Assigning meanings to programs. Mathematical Aspects of Computer Science (19-32), 1967, 10: 978-994.

[3] Hoare C A R. An axiomatic basis for computer programming. Communications of the ACM, 1969, 12(1): 53-56.

[4] Needham R M. Using Encryption for Authentication in Large Networks of Computers. New York: ACM Press, 1978.

[5] Denning D E. Timestamps in key distribution protocols. Communications of the ACM, 1981, 24(8): 533-536.

[6] Clarke E M. Design and synthesis of synchronization skeletons using branching time temporal logic. Lecture Notes in Computer Science, 1981, 131: 52-71.

[7] Dolev D, Yao A. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[8] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1989, 23(5): 1-13.

[9] Brackin S H. A HOL extension of GNY for automatically analyzing cryptographic protocols//Proceedings of the IEEE Computer Security Foundations Workshop, Kenmare, 1996.

[10] Denker G, Millen J. CAPSL integrated protocol environment//Proceedings of the IEEE DARPA Information Survivability Conference and Exposition, Hilton Head, 2000.

[11] 申宇铭, 王驹, 唐素勤. 描述逻辑 ELU 概念及术语公理集的表达能力刻画. 软件学报, 2014, 41(8): 206-210.

[12] 黄振华. 基于 Institution 理论的结构化转换系统的研究. 南京: 南京航空航天大学, 2015.

[13] 刘海, 彭长根, 张弘, 等. 一种理性安全协议的博弈逻辑描述模型. 计算机科学, 2015, 42(9): 118-126.

[14] 邓少波, 黎敏, 曹存根, 等. 具有模态词□φ=□_(1φ)∨□_(2φ)且可靠与完备的公理系统. 软件学报, 2015, 26(9): 2286-2296.

[15] 马明辉, 王善侠, 邓辉文. 极小非正规时序逻辑的矢列式演算系统. 中国科学: 信息科学, 2017, (1): 35-50.

[16] 冉婕, 谢树云, 漆丽娟. 基于时序描述逻辑的 UML 顺序图形式化研究. 计算机系统应用, 2018, 27(8): 280-284.

[17] Zadeh, Lotfi A. A note on modal logic and possibility theory. Information Sciences, 2014, 279: 908-913.

[18] Larsen K G, Mardare R. Complete proof systems for weighted modal logic. Theoretical Computer Science, 2014, 546: 164-175.

[19] Takács P, Vályi S. An extension of protocol verification modal logic to multichannel protocols. Tatra Mountains Mathematical Publications, 2015, (41): 153-166.

[20] Libal T, Volpe M. Certification of prefixed tableau proofs for modal logic//The 7th International Symposium on Games, Automata, Logics and Formal Verification, Catania, 2016.

[21] Belardinelli F, van der Hoek W. A semantical analysis of second-order propositional modal logic//The 30th AAAI Conference on Artificial Intelligence, Phoenix, 2016: 886-892.

[22] Hulst A C V, Reniers M A, Fokkink W J. Maximally permissive controlled system synthesis for non-determinism and modal logic. Discrete Event Dynamic Systems, 2017, 27(1): 109-142.

[23] Fu Y. Theory by process//International Conference on Concurrency Theory, Paris, 2010.

[24] 陈双双, 方宗德, 刘岚, 等. Pro/E 二次开发在模型检查技术中的应用. 计算机仿真, 2013, 30(8): 250-253.

[25] 阚双龙, 黄志球, 陈哲, 等. 使用事件自动机规约的 C 语言有界模型检测. 软件学报, 2014, 25(11): 2452-2472.

[26] 赵岭忠, 翟仲毅, 钱俊彦, 等. 基于关键迹和 ASP 的 CSP 模型检测. 软件学报, 2015, 26(10): 2521-2544.