高等院校信息安全专业规划教材

网络安全协议的形式化分析与验证

- 安全协议及其形式化技术的基本概念、原理和方法
- 安全协议的形式化分析方法
- 安全协议的形式化设计技术
- 形式化技术在复杂安全协议分析中的典型应用

提供电子教案

主编 李建华
参编 张爱新 薛质 李生红

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

网络安全协议的形式化分析与验证

主编　李建华
参编　张爱新　薛 质　李生红

机械工业出版社

信息安全是关系到国家安全和经济发展的重大战略问题，至关重要。安全协议作为实现信息安全的基础，其自身的安全性问题已成为安全研究的重要内容。目前，针对安全协议的安全性验证已形成了许多不同的流派、理论和方法。本书概述了形式化技术在网络安全协议分析、验证中的主要应用原理及现状；在此基础上详细地叙述了网络安全协议的形式化分析技术、形式化设计技术；最后重点介绍了目前的形式化分析技术对当前典型应用环境下复杂、实用网络安全协议的分析成果，包括IPSec协议、SSL协议、电子商务协议、移动通信安全协议及群组通信安全协议等。本书理论与应用并重，深入浅出地介绍了各类形式化分析技术的基本原理及其在大型复杂安全协议分析中的实际应用。

本书可作为信息安全专业高年级本科生教材，也可作为高等学校电子信息类、计算机类等相关专业的参考书。

图书在版编目（CIP）数据

网络安全协议的形式化分析与验证/李建华主编. —北京：机械工业出版社，2010.3

（高等院校信息安全专业规划教材）

ISBN 978-7-111-29726-0

Ⅰ. ① 网… Ⅱ. ① 李… 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（2010）第023131号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）

责任印制：乔 宇

北京京丰印刷厂印刷

2010年4月第1版·第1次印刷

184mm×260mm·14.25印张·348千字

0001－3000册

标准书号：ISBN 978-7-111-29726-0

定价：27.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

社服务中心：（010）88361066

销 售 一 部：（010）68326294

销 售 二 部：（010）88379649

读者服务部：（010）68993821

网络服务

门户网：http://www.cmpbook.com

教材网：http://www.cmpedu.com

封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出 版 说 明

信息技术的发展和推广，为人类开辟了一个新的生活空间,它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1）作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2）系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3）系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4）注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5）内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

随着以 Internet 为代表的信息化浪潮席卷全球，信息技术的应用日益普及和广泛，但 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全也提出了更高的要求，信息安全已成为关系到国家安全和经济发展的重大战略问题。

安全协议（也称密码协议）是一个分布式算法，它规定了两个或多个通信主体在一次通信过程中必须执行的一系列步骤。安全协议利用密码技术实现开放网络环境下的安全通信，达到信息安全的目的，广泛地应用于身份认证、接入控制、密钥分配、电子商务等领域。因此，安全协议作为实现信息安全的基础，其自身的安全性问题已成为安全研究的重要内容。

由于网络安全协议的重要性，从 1978 年第一个安全协议（Needham-Schroeder 协议）诞生以来，人们对它的分析和设计就一直没有停止过，也做出了卓有成效的工作。最初，人们基于经验和单纯的软件测试，采用攻击检验方法来分析其安全性。由于安全协议往往运行在复杂的、不安全的网络环境中，同时，新的攻击方法层出不穷，产生的错误很难完全由人工识别。因此，很难保证对协议安全性分析的准确性。人们一致认为，必须采用形式化的方法和工具来分析密码协议的安全性，即采用数学或逻辑模型，通过有效的程序来分析系统及其条件，以此确定一种在系统满足条件情况下所得的证明是否正确的数学理论和方法。形式化方法在网络安全协议分析中的作用主要体现在：①能使分析概念清晰；②能发现协议设计中的错误；③能证明协议的正确性；④能作为安全协议自动化分析、设计技术的理论指导。

最先提出采用形式化方法分析密码协议的是 Needham 和 Schroeder。然而，在这一领域中第一项探索性的工作是由 Dolev 和 Yao 完成的，随后由 Dolev、Even 和 Karp 在 20 世纪 70 年代后期和 80 年代初开发了一系列多项式时间算法来确定密码协议的安全性。自 1983 年 Dolev-Yao 形式化模型提出以后，密码协议形式化方法的研究有了长足的发展，到目前为止已形成了两大流派，并且出现了理论融合的趋势。一种流派称为计算流派，它基于一个详细的计算模型，安全性推理通常是通过构造一个“归约为矛盾”类型的证明得到的，这里的“矛盾”是指计算复杂性领域中一个困难问题的有效解。随机预言机模型（ROM）作为该流派的代表，对于分析密码算法的安全性有着公认的、广泛的应用。另一流派称为逻辑符号流派，它基于简单而有效的形式化语言方法，对公理的应用可以基于逻辑证明、定理证明或状态搜索技术。本书着重讨论逻辑符号流派的主要工作。目前，形式化理论在安全协议验证中的应用主要集中在形式化分析、形式化设计及自动化工具开发 3 个方面。同时，随着密码技术的不断发展和安全应用需求的不断扩大，安全协议的结构也越来越复杂化，这些都对现有的形式化协议分析技术提出了很大的挑战。

为此，面向信息安全专业的本科生，针对安全协议的形式化分析编写一本理论性与实用性兼顾的教材很有必要。本书正是为了适应这种现状需求而产生的，主要包括以下部分：

1）介绍了安全协议的基本概念以及形式化技术的基本原理与方法，这是进行安全协议形

式化分析的基础。

2）详细介绍了各类安全协议的形式化分析方法，包括基于模态逻辑技术、模型检测技术和定理证明技术的分析方法。

3）介绍了形式化技术在安全协议设计领域的主要进展，如合成协议模型、Fail-Stop 概念和 BSW 简单逻辑等。

4）分别介绍了目前得到广泛使用的复杂安全协议，如 IPSec/IKE 协议、SSL 协议、电子商务安全协议、移动通信安全协议和群组通信安全协议等，并对其安全性分析成果进行了总结。

本书共分 9 章，其中：

第 1 章详细阐述了采用形式化方法对网络安全协议进行分析的必要性，介绍了安全协议的基本概念、形式化技术基础及形式化方法在安全协议验证中的应用。

第 2 章详细介绍了基于模态逻辑技术的安全协议分析方法，以 BAN 逻辑、类 BAN 逻辑和非单调逻辑等分析逻辑为例，阐述了基于模态逻辑技术的安全协议分析思路及主要流程。

第 3 章以通信进程方法（CSP）、NRL 协议分析器、模型检测工具 Murφ、协议分析工具 BRUTUS 为例，详细阐述了基于模型检测技术的安全协议分析方法。

第 4 章具体介绍了基于定理证明的安全协议分析方法，内容涉及 Paulson 归纳法、Schneider 阶函数、串空间理论、重写逼近法和不变式产生技术。

第 5 章主要介绍了典型的安全协议形式化设计方法，包括合成协议模型及其安全性、Fail-Stop 协议概念以及 BSW 简单逻辑等。另外，基于串空间理论的认证测试方法也被广泛应用于安全协议的设计中，本书从内容完整性角度考虑，在第 4 章中对其进行了介绍。

本书从第 6 章开始，以实际应用为重点，详细总结、归纳了现有形式化分析技术在实用复杂安全协议分析中的应用成果。

第 6 章以 IPSec/IKE 协议为主要研究对象，介绍了采用扩展 BSW 逻辑、NRL 协议分析器及扩展串空间理论对其进行分析的主要过程和相关安全性结论。

第 7 章针对电子商务协议的安全性需求，详细介绍了 SSL 协议和 SET 协议，并分别采用 BAN 逻辑和 Kailar 逻辑对其安全性进行了分析验证。

第 8 章针对移动通信环境，分别介绍了 AUTLOG 认证逻辑及认证测试方法在移动通信安全协议中的分析应用。

第 9 章主要研究群组通信环境下的网络安全协议，详细介绍了利用改进的串空间理论及认证测试方法对群组密钥交换协议的分析过程及改进思路。

本书由李建华统稿及定稿，张爱新、薛质、李生红参加了部分编写工作。

王鹏、张保稳、李琳、张继昊和高奎参与了本书的部分校对工作，李谢华、蒋睿、俞扬、黄毅、田园、徐庆、张志远、战科宇、蒋呈明、田磊、张力等协助收集、整理了部分资料，在此一并表示感谢。

由于编者水平有限，书中难免存在缺点和错误，殷切希望广大读者批评指正。

编　者

目　　录

第1章 绪 论

1.1 安全协议概述

信息安全最基本的目标是实现信息的机密性，保证数据的完整性，实现身份或信息的鉴别性，具有不可抵赖性，对信息的授权和访问控制以及保证信息资源的可用性等。信息在开放的网络环境中传输会遭到各种各样的攻击，如偷听攻击、截取攻击、伪造攻击和篡改攻击等。这些攻击的存在不同程度地损害了网络用户的利益。因此，网络安全直接关系到信息系统安全，是整个信息基础结构的安全基础。为了维护开放网络环境的安全，人们广泛地使用了密码技术和安全协议。密码技术的主要功能是提供安全的服务，通过使用密码算法对消息明文进行加密以保证消息本身的安全性。它是网络安全的基础，但网络安全不能仅靠安全的密码算法实现，还需要完善的安全协议保证通信过程的安全可靠。安全协议是一个分布式算法，它规定了两个或多个通信主体在一次通信过程中必须执行的一系列步骤。安全协议利用密码技术实现开放网络环境下的安全通信，达到信息安全的目的，广泛地应用于身份认证、接入控制和密钥分配等领域。因此，安全协议作为实现信息安全的基础，其自身的安全性问题已成为安全研究的重要内容。目前，针对安全协议的安全性验证已形成了许多不同的流派、理论和方法。

另一方面，安全协议的设计是一项非常复杂而困难的工作，许多在设计时被认为是安全的协议，后来都被发现存在安全漏洞，而且采用不同的分析方法和工具，可能发现的漏洞也不大一样。如果在协议设计之初就能够避免漏洞，设计出满足安全属性要求的协议，不仅可以节约研发成本，提高研发效率，同时也避免了再度开发，这将极大地提高网络应用的安全性，避免许多重复性的工作。因此，安全协议的设计越来越受到关注。目前对安全协议设计的研究仍十分欠缺。安全协议的设计是当前安全协议研究中的一个重要领域。

安全协议的形式化方法经过长期的研究已经具备了比较完整的理论体系和模型，但目前对安全协议的分析和设计大都使用人工完成，不仅效率低，更重要的是会人为地带入一些误差，造成安全协议的分析设计结果可信度降低，甚至导致失败。考虑到人工分析和设计安全协议所造成的种种弊端，自动化的协议分析和设计工具逐渐成为协议研究的另一个重要领域。目前已经开发实现了一些安全协议自动化分析设计工具，比较常用的工具有NRL协议分析器、认证协议自动分析器（Automatic Authentication Protocol Analyzer，AAPA）等。因此，如何将成熟的形式化模型用于安全协议的自动化验证和设计，提高安全协议设计分析的效率，也是近几年国内外学者研究的重要方面。

1.1.1 安全协议的基本概念

协议是指两个或者两个以上的参与者为完成某项特定的任务而采取的一系列步骤。这个定义包含以下3层含义：

1）协议自始至终是有序的过程，每一个步骤必须执行，在前一步没有执行完之前，后面的步骤不可能执行。

2）协议至少需要两个参与者。

3）通过协议必须能够完成某项任务。

同样，安全协议是由参与通信的各方按确定的步骤做出一定的通信动作完成的，这些通信动作实现了通信本身，而动作的内容则隐含了一些密码学变换算法的实施。这些密码学变换算法，从数学上提供了达到一定程度的通信安全的基本机制。使用密码学技术的网络安全协议又称为密码协议。密码协议的目标就是通过正确使用加解密技术来解决网络通信的安全问题。这些安全问题主要表现为实现信息的机密性、保证数据的完整性、实现身份或信息的鉴别性、具有不可抵赖性、对信息的授权和访问控制以及保证信息资源的可用性等。安全协议的目标集合构成密码协议的安全属性（Security Attributes）集。它们可归纳为认证性（Authenticity）、保密性（Secrecy）、完整性（Integrity）、不可否认性（Non-Repudiation）、公平性（Fairness）、匿名性（Anonymity）、可用性（Usability）、可追究性（Accountability）和原子性（Atomicity）等。通常情况下，一个安全协议需要提供的特性和服务只是以上安全属性集的子集，这取决于其具体的应用环境。通常说一个协议是“安全”的，只是指它对于某些给定的精确定义过的性质是正确的；或者只是在某些假设环境中，对某几类特定的威胁是安全的，不存在“绝对安全”、“绝对正确”的安全协议。下面对几类重要的安全属性作一简要介绍。

1．保密性

根据应用环境的不同，保密性有不同的含义。从严格意义上说，保密性是指入侵者无法发现合法用户的任何活动，如无法做任何流量分析、不能推断消息格式和不能得到消息内容等。换言之，系统中高级用户的活动不会对系统的低级用户或外部观察者产生任何明显的影响。这是一个非常严格的定义，而且需要精确的执行过程。对大多数应用而言，保密性的目的是保护消息在传输过程中不会泄露给非授权拥有此消息的人。实现安全协议保密性的最直接方法是对机密信息进行加密。加密将明文转换为密文，在开放的网络环境中传送的是对机密信息加密后得到的密文。经授权可拥有此机密信息的协议参与者拥有相应的解密密钥，对密文解密后即可获得此机密信息；而非授权拥有者由于没有对应的解密密钥，因而即使他知道消息的格式，也无法得到消息的内容。

2．认证性

认证性是最重要的安全性质之一，因为所有其他安全性质的实现都依赖于此性质的实现。简单地说，认证是一个过程，通过这个过程，一个主体向另一个主体证明某种声称的性质。认证可细化为 3 个方面的内容，即消息源认证、实体认证以及认证的密钥建立。其中，消息源认证是指消息的接收者能验证消息所声称的源地址是其真正发出的地址，并进一步确认发出消息的时间值没被篡改过；实体认证用于验证主体身份的真实性，即验证某个主体声称的身份是否与其真实身份一致。数据源认证机制是实现实体认证的一种有效方法。认证的密钥建立通常与实体认证过程密切相关。主体间进行实体认证的目的在于能够进行安全通信，而密钥是安全信道的基础，所以在主体进行安全通信之前，通常也需要密钥建立过程（也称为密钥交换或密钥协商）。

3．完整性

完整性的含义通常是指数据不能被篡改，或者至少针对数据的任何篡改都能被检测出来，

其目的是保护消息不被未授权地篡改、删除或替代。完整性可以理解为在储存的数据上再加上一层防止篡改的保护层。封装和签名是保护完整性的常用方法。消息发送者利用密码机制或者 Hash（哈希）函数产生一个消息摘要附在传送的消息上，作为验证消息完整性的依据，称其为完整性校验值（ICV）；消息接收者在接收到消息及其完整性校验值后，将根据与发送者协商好的一系列规则，利用完整性校验值来检验所接收到的消息的完整性。因为如果消息在传输过程中被篡改的话，接收者计算出的校验值将不同于他所接收到的、由消息发送者计算的校验值。

4．不可否认性

对于大多数的安全目标我们总是假定合法用户是诚实可信的，即认为他们会遵守协议规定的操作。而不可否认性主要是考虑如何保护通信的一方不被对方欺骗，因此不再假设“合法”用户不会进行欺骗活动，在协议执行过程中能够为用户提供证据，来证明协议中某些步骤确实发生过，而且这些证据是不可伪造的。比如，发送者不能对自己发出了某条消息这一事实进行抵赖，同时接收者也不能对自己接收了某条消息这一事实进行否认。不可否认性是电子商务协议的一个重要性质，是保证交易正常进行的必要条件。保证不可否认性最常用的技术是数字签名。

5．公平性

公平的目的在于确保协议参与各方的地位和作用平等，参与各方所拥有的能力也是相同的。公平性常被用于电子商务、电子选举和电子投票事务当中。对公平性可以直观地理解为在协议运行的任何时刻每一个参与者都不会得到特别的好处。或者说，没有一方可以得到自己要的证据却可以避免另一方得到相应的证据。

比如在电子商务应用中，在一个协议消息交换开始前，交易双方（或多方）已就将要交换的项达成了一致。一个合法的参与方能按照协议规范产生消息并根据某些特定的消息推导规则处理消息；又如在电子合同签名中，我们将希望避免其中的任何一个用户通过半途停止执行协议来获得比另一方更多的利益。很多方面的协议都要求考虑这一点。为此，有些协议引入了可信第三方（公正人），其他协议则相应增加了某种形式的承诺机制。前者需要一个额外的可信实体能被访问，后者则往往需要来回传送大量的消息。

6．匿名性

匿名性是指保证消息接收者不知道发送者的身份。这个特定的属性在许多应用中都有所需求。例如，在电子选举中，投票者不希望投出的选票与自己的身份有任何联系。又如，电子商务系统也应确保交易的匿名性，防止交易过程被跟踪，保证交易过程中的用户不把个人信息泄露给未知的或不可信的个体，确保合法用户的隐私不被侵犯。

直观上看，一个在某个事件集 E 匿名的系统将拥有的特性为：当事件集 E 中的一个事件发生时，从观察者的角度看，即使他可以推断出发生了事件集 E 中的一个事件，他也不能确定是哪个事件。

7．可用性

可用性是指在适当的假设下确定协议能够达到某些预定的目标。当然，对于一个必须保证这些特性的系统而言，需要将入侵者的能力限定在某个范围内，不允许攻击者有破坏消息的无限能力。

8．可追究性

可追究性是指协议参与的各方必须对自己的行为负责，在协议执行完毕后，参与协议的任何一方主体必须提供充分的证据以解决今后可能出现的纠纷。比如，一个设计正确的电子商务协议必须遵循可追究性的原则，当电子商务交易发生纠纷时，可通过历史信息获取交易当时的情况，从而获得解决交易纠纷的能力。

9．原子性

目前，原子性主要体现在电子商务协议中。事务的原子性是数据库最基本的概念之一。T .D.Tygar 于 1996 年在电子商务中引入了原子性的概念，以规范电子商务中的资金流、信息流和物流。Tygar 定义的原子性分为以下 3 级，并且后者包含前者。

（1）钱原子性

钱原子性定义为电子商务中的资金流守恒，即资金在电子商务的各参与方的转移中既不会创生也不会消失。例如，购买者减少的钱等于销售者增加的钱。

（2）商品原子性

首先，满足商品原子性的协议一定满足钱原子性；其次，必须保证消费者一旦付了款就一定能拿到商品，不存在消费者拿了商品未付款或付了款却未得到商品的情况，这也是传统商业中“一手交钱，一手交货”的规矩。

（3）确认发送原子性

首先，满足确认发送原子性的协议就一定满足钱原子性和商品原子性；其次，需要对客户订购和商家销售的商品的内容及质量进行确认，既保证消费者在付款后商家就发送商品，也保证商品的内容及质量与消费者和商家事先协商的内容及质量保持一致。在电子商务中确认发送原子性对于数字商品（如软件、娱乐服务等）有特别重要的意义。总之，一个协议的原子性是指在任何情况下，交易完成了正确的金额，交换了正确的物品，或者当交易取消后就不存在金额与物品的交换。

1.1.2 安全协议的缺陷分析

评估一个安全协议是否安全就是检查在某种应用环境中，协议设计所要达到的安全属性是否会遭到攻击者的破坏。网络通信环境是安全协议运行的物理基础，在分布式环境中运行安全协议的最大问题在于这个通信环境存在许多未知的、不确定的、不安全的因素，攻击者无时无刻不存在，手段和能力无法具体估计和量化，刻画安全协议的运行环境和形式化描述攻击者的能力比较困难。安全协议运行环境的异常复杂性也是导致安全协议的设计和分析比较困难的原因之一。安全协议的形式化分析最主要的问题在于评价和模拟这个环境，对网络中存在的攻击者的模型具体化。

如果将安全协议及其所处的环境视为一个系统，那么在这个系统中，一般包括发送和接收信息的诚实主体和一个攻击者（把所有的攻击者都看做一个团伙），以及消息发送和接收的规则，如图 1-1 所示。协议的合法消息可被攻击者截取、重放和篡改，攻击者可进行的操作至少包括级联、拆分、加密和解密。

归纳起来，攻击者的行为能力一般表现为以下几种形式：

1）猜测协议中传递的消息。

2）转发消息到其指定的接收者处（如完整转发、篡改转发、加密后转发和解密后转

发等）。

3）延迟消息的准时送达。

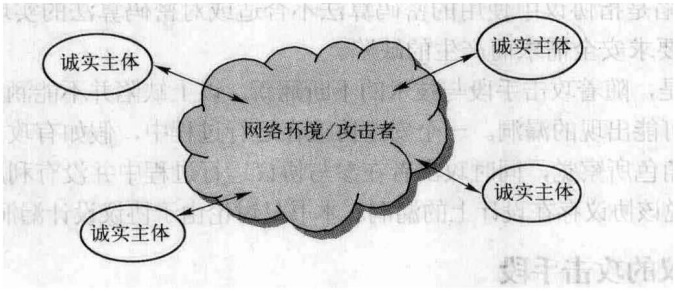

图 1-1　安全协议系统模型

4）将消息与以前接收的消息合并。

5）阻止消息被准确地送达目的地，如改变部分或全部消息的目的地等。

6）将以前接收的消息重放。

由此可见，确保安全协议的安全运行是极为重要的，但是安全协议的安全性是一个很难解决的问题，如果一个安全协议的安全性不能得到保证，我们就说该协议存在安全缺陷或安全攻击。许多广泛应用的安全协议后来都被发现存在安全缺陷。由于实际应用的安全协议产生缺陷的原因是多种多样的，对安全协议的攻击方式也各不相同，所以很难用一种通用的分类方法将安全协议的安全缺陷进行分类。S.Gritzalis 和 D.Spinellis 根据安全缺陷产生的原因和相应的攻击方法将安全缺陷分为以下 6 类。

1．基本协议缺陷

基本协议缺陷是指在安全协议的设计中由于没有或者很少防范攻击者的攻击而引起的协议缺陷。

2．口令/密钥猜测缺陷

这类缺陷产生的原因是用户往往从一些常用的词中选择口令，从而导致攻击者能够进行口令猜测攻击；或者用户选取了不安全的伪随机数生成算法构造密钥，使攻击者能够恢复该密钥。口令猜测攻击既可在线进行，也可离线进行。

3．陈旧消息缺陷

陈旧（Stale）消息缺陷主要是指协议设计中对消息的新鲜性没有充分考虑，从而使攻击者能够进行消息重放攻击，包括对消息源的攻击和对消息目的的攻击。

4．并行会话缺陷

并行会话缺陷是指协议对并行会话攻击缺乏防范，从而导致攻击者通过交换适当的协议消息能够获得所需要的信息。根据协议主体与其角色之间的对应关系，并行会话攻击可分为并行会话单角色缺陷和并行会话多角色缺陷。在单角色协议中，协议主体具有单一角色，即协议主体与其角色之间有一一对应关系；而在多重角色协议中，协议主体具有多重角色，即协议主体与其角色之间是一对多的关系。

5．内部协议缺陷

内部协议缺陷是指协议的可达性存在问题，协议的参与者中至少有一方不能够完成所有