维普资讯 http://www.cqvip.com

一种电子商务协议原子性的模型检验分析方法*)

董荣胜　郭云川　古天龙
(桂林电子工业学院计算机系　桂林541004)

摘　要　提出了一个分析电子商务协议的形式化模型,介绍了基于该模型的电子商务协议原子性的描述方法。同其他模型相比,该模型能较好地分析具有多个实例并发运行时电子商务协议的原子性。最后基于该模型,用符号模型检验工具(SMV)分析了 Digicash 协议和 Netbill 协议。

关键词　电子商务协议,模型检验,原子性

Model Checking Analysis for Atomicity of Electronic Commerce Protocol

DONG Rong-Sheng　GUO Yun-Chuan　GU Tian-Long
(School of Computer Science,Guilin University of Electronic Technology,Guilin 541004)

Abstract　A simple model for modeling electronic commerce protocol is proposed and a novel technique for formally describing its atomicity is presented. The model can be used to analyze atomicity and adapted to meet the situation that more than one instances of protocols run concurrently. Taking the protocols Digicash and Netbill as the examples,the paper presents the method how to implement the model based on the symbolic model verifier-SMV.

Keywords　Electronic commerce protocol,Model checking,Atomicity

1　引言

电子商务协议的设计是一项相当复杂且容易出错的工作,一个貌似良好的协议可能存在重大的安全漏洞。因此必须对所设计的协议进行检验。目前主要的检验方法有:1)实际攻击测试;2)形式化的检验分析技术[1]。其中形式化技术更是主要的检验手段。目前对电子商务协议分析和检验的形式化技术主要有模态逻辑(如 Kailiar 逻辑[2])、模型检验[3]和定理证明[4]。逻辑分析需要初始假设,以及对协议进行理想化,然而一旦初始假设或理想化出错,逻辑分析也无从谈起[5,6],而模型检验有助于克服这些缺点。使用模型检验方法对协议进行分析时,首先需要对协议进行建模,然后采用某种方式(通常采用时态逻辑)对协议的性质进行描述,最后通过模型检验器判断所建立的模型是否满足所希望具有的性质,其缺点是容易出现状态爆炸问题。

原子性是电子商务协议应具备的一个重要性质,针对具有多个实例并发运行时电子商务协议的原子性,本文提出了一个分析该类性质的电子商务协议的形式化模型,该模型在一定程度上降低了以往该类性质验证的繁杂程度。

2　电子商务协议模型及原子性描述

T. D. Tygar 在电子商务中引入了原子性[10,11]的概念,以规范电子商务中的资金流、信息流和物流。T. D. Tygar 将原子性分为3级:

1. 钱原子性,即,要求电子商务中的资金流守恒;

2. 商品原子性,即,要求在钱原子性的基础上保证购买者如果付了款就一定会得到商品,购买者如果得到了商品则一定付了款,不存在付了款而得不到商品或者得到了商品而未曾付款的情况;

3. 确认发送原子性,即,要求在钱原子性和商品原子性的基础上保证对客户购买的和商家销售的商品的内容及品质的双方确认。

采用模型检验方法对协议进行分析,有以下4个过程:1)建立协议模型;2)将协议模型转化为某种特定模型检验语言支持的协议模型;3)用这种特定模型检验器所支持逻辑对待检验的性质进行描述;4)运行并判断协议是否满足要求。

当模型检验器判断出协议不符合要求时,需要考虑的问题是:上述过程的前3步是否出错误,或是协议的确不满足其必须具备的性质。根据文[7]和以往的经验,这几种情况可能同时存在,从而使得模型检验的程序调试过程过于繁杂。在使用本文给出的这种方法时,如果模型检验器生成反例时,则只需要考虑:

1)将协议模型转化为某种特定模型检验语言支持的协议模型的过程是否出错;2)协议的确不满足协议必须具备的性质。

下面介绍本文提出的分析电子商务协议原子性的协议模型。

2.1　协议模型

定义1　交易主体的模型可用通信有限状态自动机(简称 CFSM)来描述,一个 CFSM 是一个五元组:

$A=(S,N,M,\delta,S_0)$

其中:S 为状态集;$N\in names$,$names$ 为所有交易主体(principal)名称集合;M 为消息集,即 $M=\{+m$ 或者 $-m \mid m\in M\}$,式中 $+m$ 表示接受消息 m,$-m$ 表示发送消息 m;$S_0\in S$,它表示初始状态;δ 为状态转移函数,$\delta:S\times M\to S$。

定义2　协议 P 是一个4元组,$P=(\Pi,C_{r_{pay}},C_{r_{goods}},C_{r_{pay}})$,其中,$\Pi$ 为协议主体 $A_1,A_2,\cdots,A_n$ 的异步复合,n 为协议主体的个数($n\geqslant 2$),协议主体 $A_1,A_2,\cdots,A_n$ 采用 CFSM $A_i=(N_i,$

*)本文得到广西自然科学基金项目(桂科字0229051)的资助。董荣胜　副教授,主要研究方向:形式化技术,安全协议工程,计算学科认知理论。郭云川　讲师,研究方向:安全协议工程,形式化技术。古天龙　教授,博士生导师,主要研究方向:形式化技术,符号模型检验,安全协议工程等。

维普资讯 http://www.cqvip.com

$S_i, M_i, \delta_i, S0_i$)来描述，其中$1 \leqslant i \leqslant n$，并且满足：

(1)每个 CFSM 的内部是同步的；

(2)各个 CFSM 之间是通过消息传递来实现通信，且通信方式是异步的。

$C_{spay}, C_{rgoods}, C_{rpay}$为3个计数器，是 $names \times names$ 到自然数$\mathbb{N}$的映射。具体定义为：

$C_{spay}(custom\_i, merchant\_j)$：主体 i(即客户 i)向主体 j(即商家 j)提交货款的次数；

$C_{rgoods}(custom\_i, merchant\_j)$：主体 i(即客户 i)收到主体 j(即商家 j)所发送商品的次数；

$C_{rpay}(custom\_i, merchant\_j)$：主体 j(即商家 j)收到主体 i(即客户 i)所提交货款的次数。

其中 $custom\_i, merchant\_i \in names$，所有的计数器的初值均为0。若客户 i 从商家 j 处收到一次商品时，$C_{rgoods}(custom_i, merchant_j)$加1，比如在 Digicash 协议中，若客户 i 从商家 j 处收到消息6，则表示客户 i 收到了货物，计数器 $C_{rgoods}(custom_i, merchant_j)$加1；若商家 j 从客户 i 处收到一次货款时，则 $C_{rpay}(custom_i, merchant_j)$加1，比如在 Digicash 协议中，若商家 j 从银行收到了消息8，则表示商家 j 从客户 i 处收到了货款，计数器 $C_{rpay}(custom_i, merchant_j)$加1；同样的方式可以给计数器 $C_{spay}(custom_i, merchant_j)$计数。

2.2 原子性描述

不同的电子商务协议有不同的支付类型，有的协议商家收到付款后再发送商品，而对于另外有些协议，客户收到了货物后再支付货款。因此对于不同的协议，其原子性的描述方式不一样，且其描述过程也是复杂的，当采用模态逻辑分析协议时，情况更是如此[7,8]。

根据钱原子性和商品原子性的要求，有：(Ⅰ)客户支付了货款当且仅当商家收到货款；(Ⅱ)客户收到了商品当且仅当客户支付了货款。

显然，原子性并不要求在协议运行的任何时刻(Ⅰ)(Ⅱ)均成立；而是要求在协议运行结束后，(Ⅰ)(Ⅱ)成立。即要求客户和商家处于初始状态的时候(因为协议运行完成之后总要回到初始状态)，(Ⅰ)(Ⅱ)成立。因此结合上面建立的分析模型，可对协议的原子性进行如下描述：

在每次完成协议运行之后，即在 CFSM 的初始状态，均要求

(R1)$C_{spay}(custom_i, merchant_j) = C_{rpay}(custom_i, merchant_j)$和

(R2)$C_{rgoods}(custom_i, merchant_j) = C_{spay}(custom_i, merchant_j)$成立。

若 $C_{spay}(custom\_i, merchant\_j) \neq C_{rpay}(custom\_i, merchant\_j)$，则表示客户支付的钱不等于商家收到的钱，即不满足钱原子性。若 $C_{rgoods}(custom\_i, merchant\_j) < C_{spay}(custom\_i, merchant\_j)$，则表示客户 i 从商家 j 处收到货物的次数小于客户 i 向商家支付货款的次数，即客户的利益受到了损失；同样的，若 $C_{rgoods}(custom\_i, merchant\_j) > C_{spay}(custom\_i, merchant\_j)$，则表示商家的利益受到了损失。即若 R2不成立，则此协议也不满足商品原子性。

3 实例分析

3.1 符号模型检验工具(SMV)介绍[9]

本文以 SMV 作为分析上述模型的工具。SMV 是在有限状态模型的基础上，检测系统属性或断言的工具。SMV 程序由两部分组成：有限状态转换系统和计算树逻辑(Computation tree logic-CTL)公式。运行 SMV 程序后，若有限状态系统满足 CTL 所描述的属性，则输出真，否则输出假，同时生成不满足属性的反例。在 SMV 系统中，系统状态集合和迁移关系都是用布尔公式隐式地表示，并在符号状态空间上进行搜索。在大多数情况下，符号化表示一个集合比显示的表示更紧凑。在 SMV 中，布尔公式用 OBDDs(Ordered Binary Decision Diagrams)来表示和操作，从而缓解了状态爆炸问题。

3.2 Digicash 协议及分析

本文主要检验 Digicash 协议的原子性，因此，在介绍 Digicash 协议过程中忽略协议加密解密过程，而将注意力集中在资金的流动和商品的转移过程上。下面是文[10]描述的忽略了加密解密过程的 Digicash 协议。

(1)$C \rightarrow B$:coin request;

(2)$B \rightarrow C$:coin;

(3)$C \rightarrow M$:goods request with blinded token;

(4)$M \rightarrow C$:challenge for the blinded token;

(5)$C \rightarrow M$:response for challenge;

(6)$M \rightarrow C$:goods;

(7)$M \rightarrow B$:blinded token,response for the challenge;

(8)$B \rightarrow M$:deposit slip。

首先，客户 C 向银行 B(下面用 C 代表客户，B 代表银行，M 代表商家)发出提款请求，B 检查提取货币的请求后，将可当钱使用的加密代币 token 发送给 C。C 收到 token 之后，如果需要在 M 处购物，那么 C 将 token 作盲变换，并将盲变换之后的 token(称为盲币)连同购物请求传送给 M。在第4步中，M 对第3步收到的盲币向 C 挑战，C 收到 M 的挑战后，在第5步对 M 的挑战做出响应。M 在收到 C 对挑战的响应并且确认该响应后，在第6步中发送商品给 C，且在第7步中将盲币以及 C 对挑战的响应发送给 B，B 确认收到的盲币是否是重复消费。若不是，则转帐给 M，并在第8步中通知 M，转账成功；若是，则 C 将被指控欺诈。

客户 C、商家 M 和银行 B 的通信有限状态自动机如图1、图2和图3所示，整个 Digicash 协议就是这3个通信有限状态自动机的异步组合。在 SMV 中，状态机内部是同步运行，状态机之间是异步组合，因此采用 SMV 能够完全模拟协议的运行。在 SMV 中，将同一类型的主体建模在同一个 Module 中，每个具体的主体都是某个 Module 的实例，每个实例用一个不同的自然数来唯一地标识，同时，该自然数也为这个主体的名称。

为了模拟协议主体欺诈和通信中断的情况，引入 Emsg 来表示混乱消息，比如客户 C 处于空闲状态 idle 时，他可以发送正确的消息 msg1，或发送混乱消息 Emsg1。需要指出是：当某个主体处于等待状态，并且收到混乱消息时，这时的状态转移应特别小心，因为这种状态的转移说明了协议对通信中断或者收到虚假消息的处理，比如客户处于接收消息2(w_msg2)状态时，若接收到混乱消息2(Emsg2)，则客户就会回到初始状态并重新发送消息1。

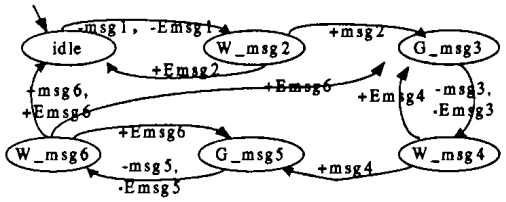

图1 客户 C 的通信有限状态自动机

维普资讯 http://www.cqvip.com

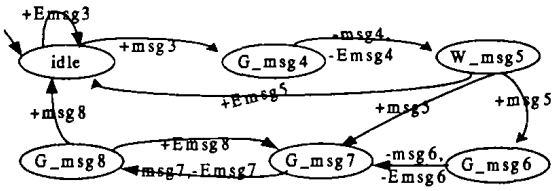

图2 商家M的通信有限状态自动机

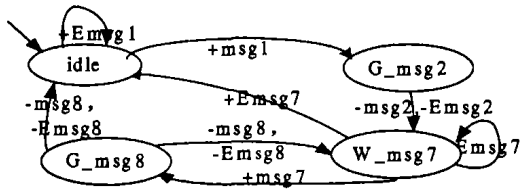

图3 银行B的通信有限状态自动机

为了分析协议的原子性，引入3个计数器 $C_{rgoods}(custom\_i, merchant\_j)$、$C_{spay}(custom_i, merchant_j)$和 $C_{rpay}(custom\_i, merchant\_j)$。下面给出描述Digicash协议原子性的CTL公式：

(A1) $AG((custom[custom\_i].state\_custom = c\_idle \ \& \ merchant[merchant\_j].state\_merchant = m\_idle) \rightarrow (custom[custom\_i].cspay[merchant\_j] = merchant[merchant\_j].crpay[custom\_i]))$

(A2) $AG((custom[custom\_i].state\_custom = c\_idle \ \& \ merchant[merchant\_j].state\_merchant = m\_idle) \rightarrow (custom[custom\_i].crgoods[merchant\_j] = merchant[merchant\_j].crpay[custom\_i]))$

其中，AG_φ为CTL公式，表示在所用路径的所有状态上，公式φ均成立。将上述协议模型转换为SMV语言。在CPU运行速度为2.6GHz，内存大小为512MB的情况下，对简化后的Digicash协议进行了分析，成功地模拟了9个客户并发地与1个商家执行协议的情况(当模拟10个客户与1个商家并发通信时，出现了状态爆炸)，结果表明Digicash协议不符合协议的原子性要求。Digicash协议不满足原子性的轨迹如图4所示(删除了一些细节)。

B的状态:	idle	g_msg2	w_msg7	w_msg7	w_msg7	w_msg7	w_msg7	g_msg8	idle
C1的计数器 crgoods:	0	0	0	0	0	0	0	0	0
C1的状态:	idle	w_msg2	g_msg3	w_msg4	g_msg5	w_msg6	idle	idle	idle
C1的计数器 crgoods:	0	0	0	0	0	0	0	0	1
M的状态:	idle	idle	idle	g_msg4	w_msg5	g_msg6	g_msg7	w_msg8	idle

图4 SMV生成的Digicash协议不满足原子性的轨迹

即：若商家发送消息6后通信中断，则客户收不到消息6，这样就会出现客户支付了钱，收不到货物，且客户无可追究商家责任的证据，这表明Digicash协议不能满足商品原子性的要求。以上分析结果与文[7]的结果完全相同。同样的方式，我们对简化后的Netbill协议的原子性进行了分析，成功地模拟了5个客户并发地同1个商家通信的情况(当模拟6个客户与1个商家并发通信时，出现了状态爆炸)，分析结果表明Netbill协议满足原子性要求，这与文[7,12]分析的结果也完全相同。

结论 本文的工作与文[3,13,14]的工作相关，文[3]提出了协调性(corresponding property)，文[13]扩展了协调性，并使认证协议的保密性和完整性得到较好的分析，文[14]利用协调性成功地模拟和分析了协议的多个实例运行的情况，并对认证协议进行了分析。本文采用类似于协调性的方式给出了原子性的描述方法，并提出了一个分析电子商务协议的形式化模型，该模型能够较好地对具有多个实例并发运行时电子商务协议原子性进行分析。

参考文献

1 Gritzalis S, Spinellis D, Georgiadis P. Security Protocols over Open Networks and Distributed Systems, formal Method for their Analysis, Design and Verification. Computer Communications, 1999, 22(8): 695～707

2 Kailar R. Accountability in Electronic Commerce Protocols. IEEE Trans. on Software Engineering, 1996, 22(5): 313～328

3 Marrero W, Clarke E, Jha S. Model checking for security protocols: [Carnegie Mellon University: Technical Report CMU-SCS-97-13 9]. 1997

4 Paulson L C. The Inductive Approach to Verifying Cryptographic Protocols. Journal of Computer Security, 1998. 85～128

5 周典萃，卿斯汉，周展飞. Kailar逻辑的缺陷. 软件学报，1999，10(12)：1238～1245

6 Boyd C, Mao W. On a limitation of BAN logic. In: Proc. of EUROCRYPT'93 Lecture Notes in Computer Science, Springer-Verlag, 1993. 240～247

7 Heintze N, Tygar J D, Wing J, Wong H C. Model Checking Electronic Commerce Protocols. In: Proc. of the 2nd USENIX Workshop on Electronic Commerce, 1996. 147～164

8 Tygar J D. Atomicity in elect ronic commerce. In: Proc. of the 15th Annual ACM Symposium on Principles of Distributed Computing, 1996. 8～26

9 周典萃，卿斯汉，周展飞. 一种分析电子商务协议的新工具. 软件学报，2001，12(9)：1318～1328

10 郭云川，古天龙，董荣胜，蔡国永. 电子商务协议形式化分析的一种新方法. 计算机科学，2004，31(8)：86～88，112

11 McMillan K L. Symbolic Model Checking. Kluwer Academic Publisher, 1993

12 郭云川，古天龙，董荣胜，蔡国永. Netbill协议原子性的符号模型检验分析. 计算机工程与应用. 2004，40(2)：57～59

13 Panti M, Spalazzi L, Tacconi S. Using the NuSMV Model Checker to Verify the Kerberos Protocols. In: Proc. of the 3rd Collaborative Technologies Symposium, 2002

14 徐蔚文，陆鑫达. 身份认证协议的模型检验分析. 计算机学报，2003，26(2)：195～201