基于分层时间有色 Petri 网的支付协议公平性分析

刘文琦 顾 宏
(大连理工大学电信学院 大连 116023)

摘 要：电子支付协议是一种重要的电子商务协议，公平性是其重要的安全属性之一。该文提出一种基于分层时间有色 Petri 网(HTCPN)的电子支付协议形式化分析方法。该方法在进行公平性分析时，充分考虑了两个环境因素：主体是否诚实和通信信道是否可靠，与其他形式化方法相比，可以更有效地分析协议公平性。使用该方法对典型支付协议 IBS 协议进行分析，分析结果验证了所提模型和方法的有效性。

关键词：有色 Petri 网(CPN)；支付协议；公平性；可追究性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)06-1445-06

Analysis of Fairness in Payment Protocols Based on Hierarchical Timed Coloured Petri Nets

Liu Wen-qi Gu Hong
(*School of Electronic and Information Engineering, Dalian University of Technology, Dalian* 116023, *China*)

Abstract: Electronic payment protocol is a kind of important electronic commerce protocol, and fairness is one of the desirable secure properties payment protocols should achieve. A new approach based on Hierarchical Timed Coloured Petri Nets (HTCPN) for modeling and analyzing fairness in payment protocols is proposed in this paper. In the analysis of fairness, it takes the honesty of principals and the reliability of communication channels into consideration. Compared with other formal methods, it can analyze fairness of protocol more efficiently. By this approach, a typical payment protocol IBS is modeled and analyzed, and the analysis result can prove the availability of the proposed model and approach.

Key words: Coloured Petri Nets (CPN); Payment protocol; Fairness; Accountability

1 引言

电子商务协议是一种保证电子商务活动正常开展的安全协议，公平性和可追究性是其最重要的性质。电子商务协议的公平性是指协议结束时，能够分别给发方和收方提供有效的对方不可否认证据；同时，在协议执行过程中的任何一步终止时，参与协议的主体处于同等的地位，任何一方都不占据优势。公平性可以确保协议参与者的利益在协议执行的任何阶段都不受到侵害。所谓可追究性，是指协议结束后发生交易纠纷时，主体可以提供必要的证据以保护自身的利益。因此，协议公平性的实现是以可追究性为前提的。支付协议是确保服务于电子商务资金流的电子支付能够有效实施的技术基础，更应保证满足公平性的要求。

形式化方法是验证各种安全协议的有效手段。近年来对电子商务协议尤其对其公平性的形式化描述和分析有影响的方法主要有基于逻辑的方法、串空间方法、进程代数方法及基于时序逻辑的方法等[1−7]。但目前还没有哪一种形式化方法能完全描述安全协议的所有性质并保证协议的绝对安全，综合使用多种方法往往能发现更多的协议缺陷和漏洞。

Petri网是一种适合描述和分析具有并行、并发和异步性质的系统的形式化工具。使用Petri网对电子商务协议的特性进行描述和动态分析，通过构造协议模型的状态空间，可以发现协议漏洞，分析协议安全性[8,9]。常用的高级Petri网有时间Petri网、时序Petri网和有色Petri网。时间Petri网[8]可描述和分析电子商务系统的实时性质，但由于在Petri网中明确地指定时间使得事件间的基本因果关系和时序关系难以表达，因此时间Petri网不适合于研究系统公平性等性质。时序Petri网[9] 描述系统的物理结构和动态行为，适合于描述和分析并发系统的时序性质，但基于时序Petri网的方法不能明确表达系统的安全性质，如主体的责任、证据的描述及不可否认性等。有色Petri网[10,11]除具备普通Petri网分析方法和技术外，还具有类型和层次结构描述能力，适合于电子商务协议性质的分析。本文使用分层时间有色Petri网对电子支付协议的可追究性和公平性进行分析。这种Petri 网方法既可以描述并分析一些其他方法不甚适合分析的协议性质，又可为电子支付协议的综合分析提供一种新的分析方法。

由于可追究性是公平性实现的基础，首先基于分层有色Petri网建立支持支付协议可追究性分析的争执仲裁一般化模型，并由此提出协议可追究性分析一般性方法。继而，抽象出包含延迟或异常终止的信息传输模型，并给出利用该模

2008-01-30 收到，2008-04-18 改回
国家 973 规划项目(2002CB312201)资助课题

型分析协议公平性的方法。最后，以一个典型支付协议IBS协议为例进行分析，发现该协议不满足公平性要求。虽然Kindred 使用RV逻辑[12]对该协议进行过形式化分析，但未能发现这个缺陷。

2 分层时间有色 Petri 网(HTCPN)

定义 一个时间有色Petri 网 (TCPN) 是一个8元组：$\mathrm{TCPN}=\{P,T;F,C,\ I_-,\ I_+,M_0,TF\}$。其中

(1) $\{P,T;F\}$ 是基网；P 是库所(Place)的有限集合，T 是变迁(Transition)的有限集合，$P\bigcup T\neq\varnothing$，$P\bigcap T=\varnothing$。$F\subseteq(P\times T)\bigcup(T\times P)$ 是有向弧(Arc)的集合，建立变迁的每种颜色与库所的颜色之间的对应关系。

(2) C 是颜色集合，当 $p\in P$ 时，$C(p)$ 是关于 P 中托肯(Token)的一个颜色集合，即托肯色集；当 $t\in T$ 时，$C(t)$ 是关于 t 的发生的一个颜色集合，即出现色集。

(3) I_-，I_+ 是输入函数和输出函数，用来确定变迁发生后库所(Place)中托肯的变化，对于所有的 $(p,t)\in P\times T$ 有

$$I_-(p,t)\in[C(t)_{MS}\to C(p)_{MS}]_L\quad(p,t)\in P\times T$$
$$I_-(p,t)=0\quad(p,t)\notin P\times T$$
$$I_+(p,t)\in[C(p)_{MS}\to C(t)_{MS}]_L\quad(p,t)\in P\times T$$
$$I_+(p,t)=0\quad(p,t)\notin P\times T$$

$C(p)_{MS}:[S\to R]_L$ 为从集合 S 到 R 所有线性函数的集合，S_{MS} 为非空集合 S 上的多重集。

(4) M_0 称为初始标识，对 $p\in P$，$M_0(p)$ 是库所 p 的颜色集合上的多重集。

(5) TF 是时间映射函数。$TF:T\to 0\bigcup Q^+$ (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，称之为瞬时变迁，不为0时称之为时延变迁。

对于复杂、庞大的模型，引入分层概念，利用结构化的设计思想采用从上到下逐步设计，通过对各个子网的模拟仿真实现对整个系统的仿真。通过各子网中的端口库所与父网中的相应库所相互融合，并把父网中与子网对应的置换变迁用子网来替代，可形成一个统一的网系统。采用分层机制的时间有色Petri网称为分层时间有色Petri网(HTCPN)。

3 公平性分析

3.1 支付系统概述

支付系统一般由三部分组成：客户(C)、商家(M)、金融机构(B)。通常还有支付网关(PG)负责连接 Internet 与银行内部支付网络系统，如图 1 所示。

C 向 M 发出支付请求，并对 PG 提出扣款请求，要求从其账户上扣除支付金额；M 向 PG 发出转账请求，要求将 C 支付的金额转移到自己帐户上；PG 将转帐请求和扣款请求提交给 B，B 验证请求信息有效后实现相应的转帐业务，并返回请求的响应信息，箭头表明信息的传递方向。

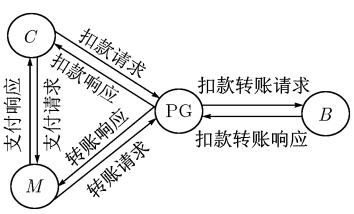

图 1 支付系统简图

3.2 公平性分析的基本思想

协议满足公平性要求：(1)协议正确执行后应满足可追究性；(2)保证参加协议的各方在协议执行的任何阶段都处于同等地位。如协议完成时，双方均可提供对方不可否认的有效证据，则协议满足可追究性。发方不可否认证据(NRO)是指收方提供消息来源的证据，以避免发方否认曾发送过消息；收方不可否认(NRR)是指消息发方提供消息收到的证据，以避免收方否认曾收到消息。当协议满足可追究性要求时，如协议执行过程中异常终止，若交易双方能同时收到或者未收到对方的不可否认证据，则协议满足公平性。

协议在运行过程中，传输信息的信道可能是可靠信道、弹性信道或不可靠信道。同时，协议的参与者为了各自的利益，可能故意拖延或拒绝信息的传输。假设可信方(如银行)向协议的其它参与者传输信息的信道是可靠信道，其余信息是在不可靠信道或弹性信道中传输的。根据以上的分析，本文所提公平性分析方法步骤如下：

(1)建立协议的有色 Petri 网模型；

(2)根据可追究性分析原则，确定协议参与者的不可否认证据。建立仲裁争执子模型，在协议基本模型的基础上，修正模型，进行协议可追究性分析；

(3)对于满足可追究性的协议，基于时间有色 Petri 网建立带有延迟特性的信息传输子模型，并将其加入到原协议模型中。

(4)分析各种异常终止情况下协议的公平性。

3.3 可追究性分析方法

根据 3.1 节所述简化的支付协议构建协议的 Petri 网抽象模型如图 2 所示。

其中变迁 t_1,t_2,t_3 和 t_4 是置换变迁，分别对应 C，M，PG 和 B 的模型子页，具体的各模型子页需根据不同协议分别进行建立。库所 p_1，p_3 和 p_4 分别是支付请求信息、扣款请求信息及转账请求信息，p_5，p_6 分别是 PG 向 B 发出的扣款转账信息及 B 对 PG 的响应信息，p_2, p_7 和 p_8 则是支付响应信息、转账响应信息及扣款响应信息。

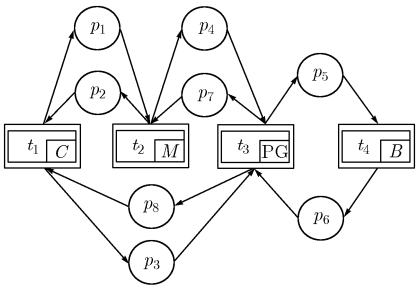

图 2 支付协议 Petri 网模型

为了分析协议可追究性，在协议中增加争执发生时认定责任的仲裁阶段，通过对各参与者提供对方的不可否认证据进行验证实现对责任的追究。不同协议对不可否认证据的提取和验证各有不同，通用的仲裁争执 Petri 网模型如图 3 所示。

颜色集 RESULT{true, false}表示状态，库所 Finish，ORes 和 RRes 的类型定义为 RESULT，库所 Finish 表示协议完成状态。库所 R_NRO 和 O_NRR 分别表示收方和发方提供的包含对方不可否认证据的信息，经 Ext_NRO 和 Ext_NRR 变迁提取出不可否认证据输出到库所 NRO 和 NRR 中，再经 Chk_NRO 和 Chk_NRR 变迁对不可否认证据进行验证，如保存验证结果的库所 ORes 和 RRes 最终都可以获得值为 true 的托肯，则表明协议完成后参与者均可以获得对方的不可否认证据，协议满足可追究性要求。

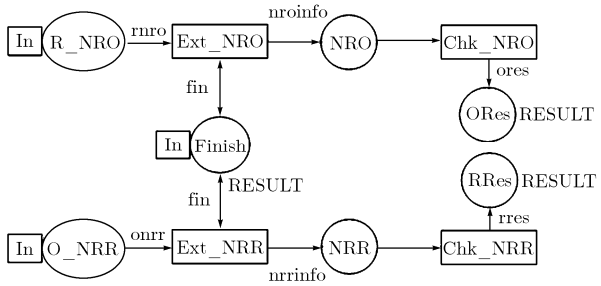

图 3 通用的仲裁争执模型

3.4 公平性分析方法

可以将不诚实参与者可能采取拖延或拒绝发送信息的行为用弹性信道或不可靠信道来模拟，各种类型的通信信道以及参与者的不诚实行为对协议产生的影响最终表现为信息传输的延迟，可根据延迟的时间长短设为：零延迟(忽略传输时间)、允许范围延迟、大延迟(超出允许范围)、无穷时间延迟(断路)。基于此，建立带有延时的信息传输模型就可以描述信息传输过程中不同类型信道的特性及参与者恶意的拖延或拒绝发送信息的行为，如图 4 所示。

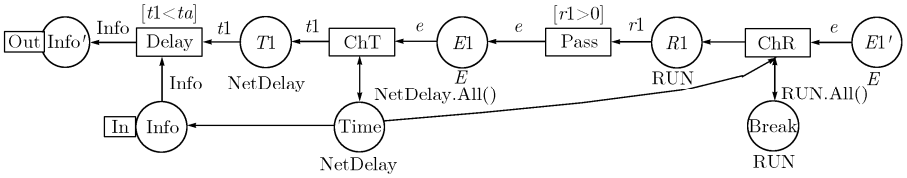

图 4 带有延时的信息传输模型

图中，定义颜色集 RUN{0, 1}表示线路通路或断路，颜色集 NetDelay{0, td, tdd}表示传输信息在信道中传输的时间，0 表示延迟时间忽略不计，td 表示允许延迟时间，tdd 表示大延迟时间。库所 Break，$R1$ 的类型定义为 RUN，表示信息传输信道状态。库所 TIME，$T1$ 的类型定义为 NetDelay，表示信息传输的延迟。变迁 ChR，ChT 表示随机选择信道通路或断路以及通路时信道的延迟时间。假设收取信息的最大允许时延为 ta($\mathrm{td} \le \mathrm{ta} < \mathrm{tdd}$)，如果信道断路，协议将终止；如通路，但收方收到消息的延迟时间为 tdd，大于最大允许时延 ta，则意味着信息延迟已超出允许时限，也终止协议；除此两种情况外，协议将正常进行。

分析协议模型的运行结果，检查所有因断路或因通信大延迟造成协议终止的状态，如果在某一状态下，某参与方获得了另一方的不可否认证据，但是对方未获得该方的不可否认证据，表明双方此时不处于同等地位，则公平性不能得到满足；反之，协议满足公平性要求。

4 应用实例

IBS 协议是美国卡内基-梅隆大学开发的电子商务协议[13]，下面采取上述方法对该协议公平性进行分析，验证本文所提模型和方法的有效性。

4.1 IBS 协议概述

该协议中包括客户 E 、商家 S 和银行 B ，协议步骤如图 5 所示。

其中：K_p, K_p^{-1}，实体 P 公钥、私钥；$\{\mathrm{Info}\}_{K_P}$，使用 P 的公钥对消息 Info 加密；$\{\mathrm{Info}\}_{K_P^{-1}}$，$P$ 对消息 Info 签名；Price，服务的价格；Service，服务的内容。分为确定价格(1–2)、提供服务(3–7)和传递发票(8–11)3 个阶段。

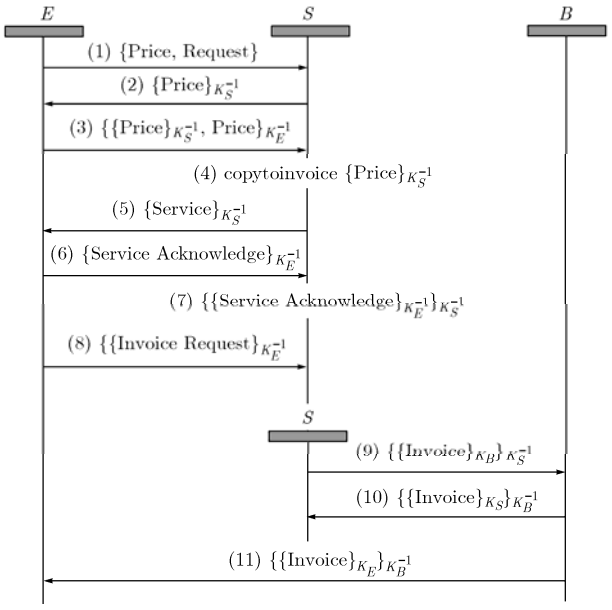

图 5 IBS 协议流程示意图

4.2 IBS 协议的 CPN 模型

IBS 协议的 Petri 网模型顶层如图 6 所示。

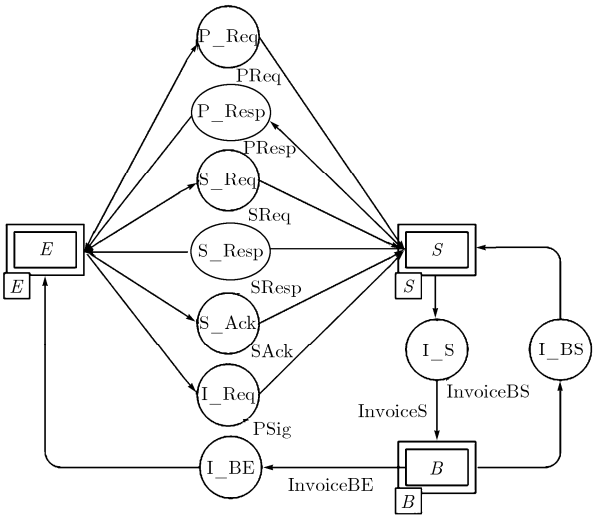

图 6 IBS 协议模型 Top 层

变迁 E, S 和 B 是置换变迁，分别对应客户 E，商家 S 和银行 B 的模型子页(本文略)。库所 P_Req，P_Resp 分别对应确定价格阶段中的询价请求信息和询价响应信息；库所 S_Req，S_Resp 和 S_Ack 分别对应服务请求信息、服务信息和获得服务的响应信息；I_Req，I_S，I_BS 和 I_BE 分别是 E 提出的发票请求信息，S 向 B 提供的发票信息，B 在转帐后返回给 S 和 E 的信息。

4.3 协议的可追究性分析

协议中的银行 B 可以看作是可信方，因此仅分析 E 与 S 之间的可追究性能否得到满足。协议中 E 和 S 之间就价格、服务和发票进行信息的交互，因此从这 3 个阶段进行分析。基于图 3 提出的仲裁一般化模型建立 IBS 协议的仲裁模型，在协议模型的 Top 层增加置换变迁 V 对应于仲裁争执的 V 模型子页。E 和 S 就价格、服务和发票阶段的执行向仲裁提供的对方不可否认证据。以提供服务阶段为例进行分析，该阶段 S 提交的 E 不可否认证据是：

$$\text{NRO}=\{\{\{\text{Price}\}_{K_S^{-1}},\text{Price}\}_{K_E^{-1}},\{\text{Service Acknowledge}\}_{K_E^{-1}}\}$$

E 提交的 S 不可否认证据是：

$$\text{NRR}=\{\text{Service}\}_{K_S^{-1}}$$

V 模型子页服务提供阶段的仲裁部分如图 7 所示。

如协议执行完毕 E 否认发出过服务请求，S 提供 E 不可否认证据经 Ver_NRO 变迁验证，库所 E-Rlt 若获得值为 true 的托肯，则意味着 S 提交的 E 不可否认证据被验证有效，E 发出过服务请求并得到了服务响应。同理，可以通过验证 E 提供 S 不可否认证据的有效性，确定 S 是否诚实。

使用 CPN Tools[14]仿真模型，下面的查询语句对协议执行结果进行查询：

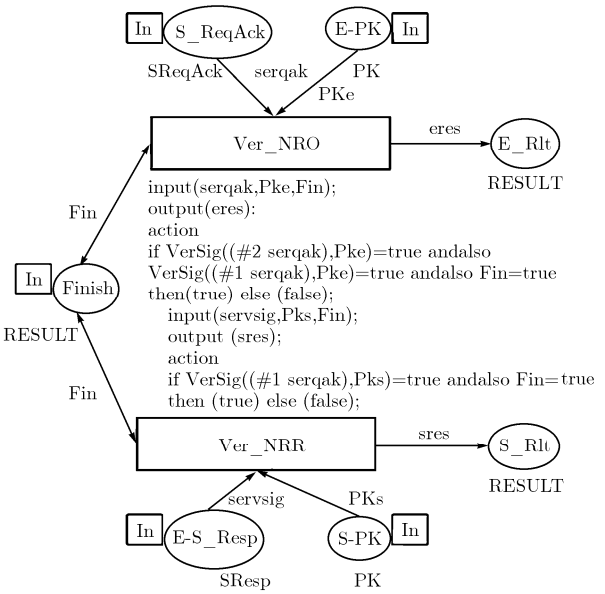

图 7 IBS 协议仲裁争执子模型服务提供阶段仲裁部分

ListDeadMarkings( )=38

(Mark.Verifier'E_Rlt 1 38, Mark. Verifier'S_Rlt 1 38)=([true], [true])

即 Verifier 子页中库所 S_Rlt 和 E_Rlt 可获得值为 true 的托肯，意味在提供服务阶段，E 和 S 都会获得对方就服务的不可否认证据。因此协议的服务提供阶段满足可追究性。

类似地，可判断价格确定阶段和发票传递阶段满足可追究性，因此 IBS 协议满足可追究性。

4.4 协议的公平性分析

假设 E 和 S 之间的 6 次信息传输以及 S 向 B 提交发票信息的传输都在弹性信道或不可靠信道上进行，B 向 E 和 S 发送扣款和转账响应的信息在可靠信道上传输，同时假设仅有 B 为可信方，E 和 S 都可能采取恶意行为拖延或拒绝信息的发送。基于 3.4 节分析，为上述 IBS 协议中的信息传输添加延时和通断参数，建立 IBS 协议信息传输子模型，如图 8 所示，顶层添加对应的置换变迁 Net，从而获得考虑通信延迟的 IBS 协议 HTCPN 模型。

使用 CPN Tools 仿真模型，对应状态空间报告表明模型中存在 64 个死节点，说明对应于不同阶段的通信，由于通信断路或信息延迟造成的协议终止状态。

分析在通信出现断路或大延迟的情况下，收、发双方是否仍能够同时获得对方的不可否认证据。以提供服务阶段为例进行分析。使用查询语句查询由于通信断路或信息大延迟而终止协议的情况下，如服务提供商 S 和客户 E 的模型子页中存放对方不可否认证据的库所中均有托肯且可以通过不可否认证据的有效性验证，或者都没有得到托肯，则说明提供服务阶段符合公平性要求，否则不符合公平性。以第(6)步 E 发送给 S 一个签名的服务认可消息的通信为例说明，使用查询语句：

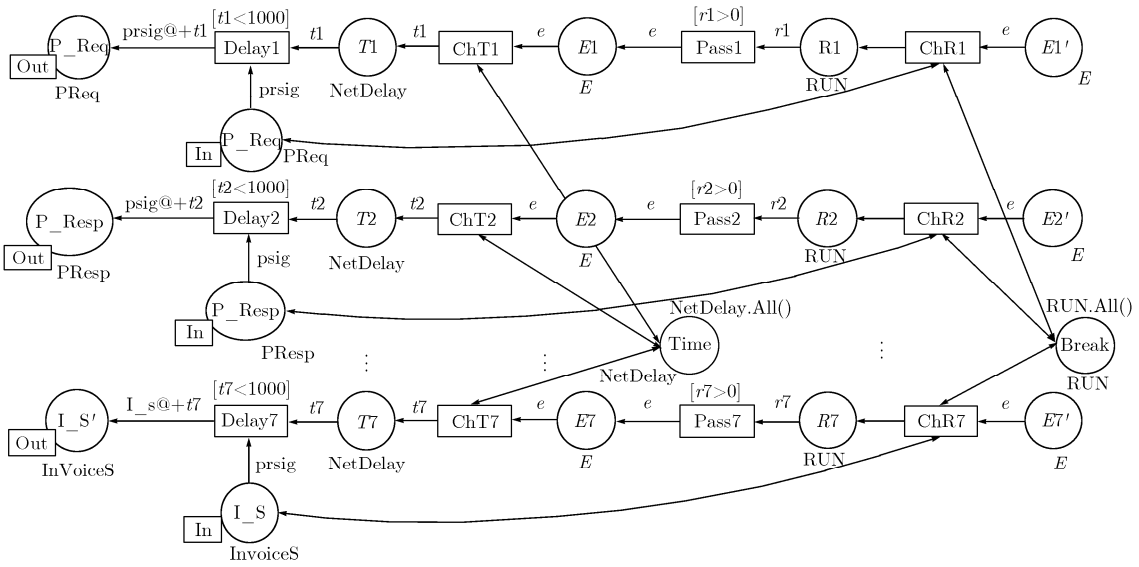

图 8 IBS 协议信息传输子模型

SearchNodes(EntireGraph,
fn n =>(Mark.Net'R5 1 n=[0] orelse Mark.Net'T5 1 n=[1000])
NoLimit,
fn n=>(Mark..S'Service_NRO, Mark.E'Service_NRR),
[ ],
op::)
得到如下查询结果：
[([ ],[(Service,SKs)@40]),([ ],[(Service,SKs)@40]),[ ],[(Service,SKs)@30]), …

从查询结果可以看出，所有符合条件的节点中，E 模型子页库所 Service_NRR 可以获得托肯而 S 模型子页库所 Service_NRO 为空，即在第 6 步因通信断路或信息大延迟造成协议异常终止的情况下，E 和 S 不能同时获得对方不可否认证据，S 在发送给 E 服务信息后却得不到 E 发出的服务认可消息，双方此时不处于平等地位，因此不满足公平性。

类似可分析其他两个阶段公平性能够得到满足，综合考虑几个阶段的分析结果，IBS 协议不满足公平性要求。

5　结束语

公平性是支付协议一种重要的安全属性，本文给出了一种采用分层时间有色 Petri 网对电子支付协议公平性进行分析的新方法。

公平性和可追究性是密不可分的，协议如果不满足可追究性要求，则一定无法满足公平性要求，本文首先设计仲裁争执模型对协议的可追究性进行分析。当协议满足可追究性，在协议 HCPN 模型的基础上，引入时间属性建立带有延时的信息传输模型，分析由于通信延迟或中断造成协议终止的各种情况下协议参与者能否保持处于同等地位，可获得协议公平性能否得到满足的结论。使用上述方法对 IBS 协议进行分析，证明 IBS 协议满足可追究性，但是不满足公平性，该分析结果验证了本方法的有效性。

电子商务协议相对协议复杂，采用基于分层有色 Petri 网的建模和分析方法可以获得规范的消息定义，简单紧凑的协议模型和有效的分析。本文着重讨论电子支付协议公平性的分析方法，由于针对其他的电子商务协议，也可类似建立争执仲裁模型和信息传输模型，因此本文所述方法也可用于其他电子商务协议的公平性分析中。

参 考 文 献

[1] Kailar R. Accountability in electronic commerce protocols [J]. *IEEE Trans. on Software Engineering*, 1996, 2(5): 313–328.

[2] 周典萃, 卿斯汉, 周展飞. 一种分析电子商务协议的新工具[J]. 软件学报, 2001, 12(9):1318–1328.
Zhou Dian-cui, Qing Si-han, and Zhou Zhan-fei. A new approach for the analysis of electronic commerce protocols [J]. *Journal of Software*, 2001, 12(9): 1318–1328.

[3] Kungpisdan S, Srinivasan B, and Le P D. Accountability logic for mobile payment protocols [C]. Proc. of the International Conference on Information Technology: Coding and Computing. Los Alamitos: IEEE Computer Society Press, 2004: 40–44.

[4] 卿斯汉. 一种电子商务协议形式化分析方法[J]. 软件学报, 2005, 16(10): 1757–1765.
Qing Si-han. A formal method for analyzing electronic commerce protocols [J]. *Journal of Software*, 2005, 16(10): 1757–1765.

[5] Kremer S and Raskin J F. A game-based verification of non-repudiation and fair exchange protocols [J]. *Journal of Computer Security*, 2003, 11(3): 399–429.

[6] 文静华, 李祥, 张焕国, 等. 基于 ATL 的公平电子商务协议形式化分析[J]. 电子与信息学报, 2007, 29(4): 901–905.
Wen Jing-hua, Li Xiang, and Zhang Huan-guo, *et al*.. Formal analysis of fair E-commerce protocols based on ATL [J]. *Journal of Electronics & Information Technology*, 2007, 29(4): 901–905.

[7] 王彩芬, 葛建华. 一种分析电子商务协议的新方法 [J]. 计算机学报, 2004, 27(4): 507–515.
Wang Cai-fen and Ge Jian-hua. A new approach for the analysis of electronic commerce protocols[J]. *Chinese Journal of Computers*, 2004, 27(4): 507–515.

[8] Jaragh M and Saleh K. Protocol specification and analysis using the fuzzy timed Petri net model [J]. *International Journal of Applied Mathematics*, 2000, 3(2): 187–208.

[9] 杜玉越, 蒋昌俊. 网上证券交易系统的时序 Petri 网描述及验证[J]. 软件学报, 2002, 13(8): 1698–1704.
Du Yu-yue and Jiang Chang-jun. Description and verification of an online stock trading system by using temporal Petri nets[J]. *Journal of Software*, 2002, 13(8): 1698–1704.

[10] Billington J, Gallasch G E, and Han B. A coloured Petri net approach to protocol verification [C]. Lectures on Concurrency and Petri Nets-Advances in Petri Nets, Heidelberg: Springer-Verlag, 2004, LNCS 3098: 210–290.

[11] Katsaros P, Odontidis V, and Gousidou-Koutita M. Colored Petri net based model checking and failure analysis for E-commerce protocols [C]. Proceedings of the Sixth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools. Denmark: DAIMI PB-576, 2005: 267–283.

[12] Kindred D. Theory generation for security protocols [D]. [Ph.D.dissertation]. Pittsburgh: Computer Science Department, Carnegie Mellon University, 1999.

[13] O'Toole K R. The Internet billing server transaction protocol alternatives[R]. Carnegie Mellon University, Information Networking Institute, Tech Rep: INITR-1, 1994.

[14] CPN Tools-help [EB/OL]. http://wiki.daimi.au.dk: 8000/cpntools-help/cpntools-help.wiki.

刘文琦： 女，1973 年生，副教授，研究方向为安全协议、电子商务.

顾 宏： 男，1961 年生，教授，研究方向为电子商务.