第34卷 第16期 计 算 机 工 程 2008年8月
Vol.34 No.16 Computer Engineering August 2008
·安全技术· 文章编号：1000—3428(2008)16—0177—03 文献标识码：A 中图分类号：TP309

基于CSP和动态博弈的电子支付系统模型

钟 旭[1]，程杰仁[2]，唐湘滟[3]，史伟奇[4]
(1. 长沙学院计算机系，长沙 410003；2. 湘南学院数学系，郴州 423000；
3. 湖南省标准化研究院，长沙 410007；4. 湖南公安高等专科学校计算机系，长沙 410006)

摘 要：分析电子支付系统的安全问题，提出基于通信顺序进程和动态博弈的电子支付系统模型。该模型对协议主体的各种不诚实行为和3种质量的通信媒介建模，可以用于分析协议主体和通信媒介之间的合作和竞争行为。对进程失效和由于消息丢失或消息延迟导致的通信失效建模，能分析各种失效情况下协议的安全属性。

关键词：公平性；电子支付协议；通信顺序进程；动态博弈；系统模型

Electronic Payment System Model Based on CSP and Dynamic Game

ZHONG Xu[1], CHENG Jie-ren2, TANG Xiang-yan3, SHI Wei-qi[4]
(1. Department of Computer, Changsha University, Changsha 410003; 2. Department of Mathematics, Xiangnan University, Chenzhou 423000;
3. Hunan Institute of Standardization, Changsha 410007; 4. Department of Computer, Hunan Public Security Academy, Changsha 410006)

【Abstract】On the basis of analyzing the features of electronic ecommerce systems, a novel electronic ecommerce systems model based on Communicating Sequential Processes(CSP) and dynamic game is proposed. Modeling channels in different qualities and participants of dishonest behaviors help to analyze cooperative and adversarial behaviors. Modeling process failure and channel failure help to analyze a protocol's security properties in failed environment.

【Key words】fairness; electronic payment protocol; Communicating Sequential Processes(CSP); dynamic game; system model

1 概述

目前电子支付系统缺乏一个通用的电子支付系统形式模型，难以应用形式化方法分析系统的安全属性。电子支付系统与纸币支付和银行专用网相比主要存在2个问题：(1)电子货币易于复制和伪造，电子支付系统缺乏安全约束。(2)电子支付系统各个协议主体之间需要通过具有安全风险的开放网络进行非面对面的信息交互，主体的分布性给电子支付带来了信任冲突。Zhou等在公平性(fairness)和非否认性(non-repudiance)研究领域有较好的研究成果[1]。Heintze等提出了三级原子性(atomicity)的概念，设计了NetBill协议，但是这些性质只是基于设计者提出的非形式化定义，缺乏准确一致的形式化定义[2]。Clarke等采用逻辑描述IKP协议的隐私性(privacy)和匿名性(anonymity)[3]。Kailar等基于逻辑推理方法分析了电子支付协议的可追究性(accountability)[4]。

电子支付系统是一种分布式的并发系统，其包含顾客、商家和银行3类主体之间的交叠行动序列以及主体与通信媒介的同步行为，顾客和商家可能会有不诚实行为。此外电子支付系统存在多个主体的联合和竞争行为，协议主体在遵守协议给定的约束情况下会最大化自己的收益，因此电子支付系统具有动态博弈的特征。通信顺序进程(CSP)是著名计算机科学家C.A.R.Hoare为解决并发现象而提出的代数理论，是一个专为描述并发系统的通信实体行为而设计的一种抽象语言，可用于网络安全协议的描述与分析[5]。该方法将安全协议的问题规约为CSP进程是否满足CSP规范。博弈论是研究2人或多人谋略和决策问题的理论[6]。参与博弈的决策主体称为参与者，通常又称为参与人或局中人。参与者参加博弈的目的是通过合理选择自己的行动，以期获取最大化自己的收益。因此本文基于CSP相关理论和动态博弈系统建立了基于CSP和动态博弈的电子支付系统模型。

2 基于CSP和动态博弈的电子支付系统模型

2.1 系统模型表示

电子支付系统模型由协议主体和通信媒介构成，如图1所示。

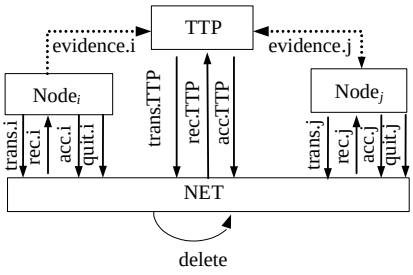

图1 基于CSP和动态博弈的电子支付系统模型

协议主体包括顾客(Node$_i$, i是自然数)、商家(Node$_j$, j是自

基金项目：国家自然科学基金资助项目(60603062)；公安部应用创新计划基金资助项目(2007YYCXHNST072)；湖南省自然科学基金资助项目(06JJ3035)；湖南省教育厅基金资助科研项目(07C718)；湖南省高校优秀青年科学研究项目(07B017)

作者简介：钟 旭(1972－)，女，讲师，主研方向：信息安全；程杰仁，讲师、在职博士研究生；唐湘滟，助理工程师；史伟奇，教授

收稿日期：2008-06-01 **E-mail：**cjr22@163.com

然数)和银行TTP。通信媒介(NET)是一类没有密码运算能力特殊的主体，主体间的连线表示通信媒介和其他主体之间的通信信道。主体诚实指主体服从协议，主体不诚实指主体违背协议。TTP是可信任第三方属于诚实主体。NET根据其传送消息的质量分为 3 类：可靠，可恢复和不可靠。NET可靠是指消息一定能在规定的时间内传送成功，NET可恢复是指消息最终将被传送成功但具体时间不能确定，NET不可靠是指消息会丢失。通信失效指消息丢失和消息延迟。本模型中采用CSP描述系统主体行为，对主体建模。

系统模型采用一个五元组$<N,Q,p,\{\mathcal{I}_i\}_{i\in N},\geqslant_i>$表示，其中：

(1)N为参与者集合。假定参与者集合N={1,2,3,4}，其中，1 是Node$_i$；2 是Node$_j$；3 是TTP；4 是NET。

(2)Q 为参与者的行动序列集合，具备以下性质：

1)空序列$\varnothing\in Q$。

2)如果 $(q_k)_{k=1}^{w}\in Q$ (q 为行动序列)且 $0<v<w$(w 是自然数)，则 $(q_k)_{k=1}^{v}\in Q$。

3)如果对任意正整数 v 都满足 $(q_k)_{k=1}^{w}\in Q$ (q 为行动序列)，则 $(q_k)_{k=1}^{\infty}\in Q$。若 $(q_k)_{k=1}^{w}\in Q$ 是无穷序列或者不存在行动 q_{w+1} 使得 $(q_k)_{k=1}^{w+1}\in Q$，称 $(q_k)_{k=1}^{w}$ 是极大行动序列，Z 表示极大行动序列集合。

(3)p: $\{Q\backslash Z\}\to N$。计算非极大行动序列的下一个行动者。

(4)$\mathcal{I}_i(i\in N)$。表示参与者i的所有信息集集合。

(5)$\geqslant_i(i\in N)$。极大行动序列关于参与者i的优先级关系。

2.2 基本定义

原子消息是指具有特定意义的最小符号串，表示主体的原子行动即事件，记为 m。原子消息集合记为 AM。电子支付系统中密码函数集合记为 F。

定义 1 消息集合 M。$M\subseteq(AM\cup F)^*$为满足以下条件的集合$\mathfrak{M}\subseteq(AM\cup F)^*$中的最小集合：

(1)若 $m\in AM$，则 $m\in\mathfrak{M}$；

(2)若$m_1,m_2\in\mathfrak{M}$，则$m_1m_2\in\mathfrak{M}$；

(3)若$f\in F$且$m_i\in\mathfrak{M}$ (i=1,2,⋯,n)，则函数f对m_i(i=1,2,⋯,n)的作用$f(m_1, m_2,\cdots,m_n)\in\mathfrak{M}$。

定义 2 消息构造算子$\vdash$。消息 m 由消息集合 M 可构造，即 $M\vdash m$，当且仅当 m 和 M 满足以下条件之一：

(1)$m\in M$；

(2)$m=m_1m_2$，且$M\vdash m_1$和$M\vdash m_2$；

(3)$m=m_i(i=1,2)$，且$M\vdash m_1m_2$；

(4)$m=f(m_1, m_2,\cdots,m_n)$，且$\forall i\in\{1,2,\cdots,n\}M\vdash m_i$。

当 2 个事件并发时，如果必须强调同时发生，那么这 2 个事件被认为是一个事件；否则按任意顺序记录 2 个事件。主体之间通过 NET 传递消息，一次消息传递用通信事件表示。通信事件是由主体和 NET 同时参与的同步事件，记为 $c.i.j.m$。其中，c 是信道名；i 表示主体；j 表示消息的接收者；m 是待传送的消息。

2.3 参与者

参与者包含顾客(Node$_i$)、商家(Node$_j$)、可信任第三方(TTP)和通信媒介(NET)。顾客期望通过电子支付购买到商品，商家期望卖出商品，由于顾客和商家可能不诚实，因此顾客和商家在博弈中存在多个策略。TTP始终服从协议，提供信任服务，没有利益需求，因此，TTP在博弈中只存在一个策略。NET负责消息传送，没有利益需求，由于NET信道质量有可靠、可恢复和不可靠 3 类，因此NET在博弈中存在多个策略。

2.4 信息集

信息集是参与者i从行动序列中获取的博弈信息，$I_i\in\mathcal{I}_i$。状态$\sum_i(q)$表示参与者i在博弈完成行动序列q后所获得的信息。$\sum_i(q)$表示为四元组$<Act_i(q), H_i(q), MS_i(q), R_i(q)>$。其中，$Act_i(q)$表示参与者$i$是否活跃，若值为 1 表示活跃，否则不活跃；$H_i(q)$表示参与者$i$发生的历史事件序列；$MS_i(q)$表示参与者$i$的消息集合，包括协议初始赋予$i$的知识，协议执行过程中$i$收到的消息集合和$i$产生的新消息；计数器$R_i(q)$表示参与者$i$博弈的次数。

2.5 可行事件

可行事件由事件可行的条件和事件对状态的更新 2 部分组成，记为a。参与者i(i=1,2)在行动序列q后的可选事件集合记为$A_i(\Sigma_i(q))(j\in N, i\neq j)$。trans事件表示参与者$i$($i$=1,2)发送其构造的消息，rec事件表示参与者接收消息，acc事件表示接受通过验证的收到消息，quit事件表示参与者在参与协议过程中主动退出协议的行为，faillocal事件表示参与者的本地进程失效用，failremote事件表示参与者能检测到的远程进程失效，evidence事件表示参与者在正常支付后没有拿到商品或发出商品没有收到支付时向可信第三方提供证据，并且发出恢复他受损利益的请求。参与者i(i=3)在行动序列q后的可选事件集合记为$A_{\mathrm{TTP}}(\Sigma_{\mathrm{TTP}}(q))$。TTP始终服从协议发送、接收和验证消息。假定TTP不会失效和中途退出协议。参与者i(i=4)在行动序列q后的可选事件集合记为$A_{\mathrm{NET}}(\Sigma_{\mathrm{NET}}(q))$。与参与者$i$($i$=1,2)不同的是NET的trans事件表示准备接收消息；rec事件表示只要消息的指定接收者活跃，NET就可以向该接收者发送消息；delete事件表示删除不可靠的NET消息事件，NET不具备密码运算能力而不要构造和验证消息。

各参与者和TTP分别通过信道trans.i和rec.i(i=1,2,3)与NET通信，如图 1 所示。一次通信事件由发起者和响应者同步完成，因此，使用主动事件和响应事件来区分两者的同一个通信事件。用谓词$valid$抽象电子货币安全性的验证过程，谓词$valid_i(m,q,cond_m)$代表的含义是 i在博弈完成行动序列q后，验证其接收的消息m是否满足谓词$cond_m$，$cond_m$是协议规定的判定m是否有效的条件。

2.6 战略

战略是参与者如何对其他参与者的行动作出反应的行动规则，它规定参与者在什么时候该选择什么行动。博弈是参与者经过多轮行动后完成。假设$P'(q,v)=\{\ k\in N'\colon Act_k=1,\ k>v\}$表示完成行动序列$q$后仍然活跃的编号大于$v$的参与者集合，$P'(q,v)$中编号最小的参与者为$k_{\min}(q,v)=\min_{k\in p'(q,v)}k$。NET消息空间的消息权值$(r,t)$是指NET在第$r$轮博弈中收到的第$t$个消息，即第$r$轮中发生的第$t$个trans事件。二元关系$'\gtrsim'$表示NET消息空间的消息被发送的优先关系。$'m_1\gtrsim m_2'$表示$m_1$在$m_2$之前被NET发送：$m_1\gtrsim m_2$，当且仅当：$r_1=r_2,\ t_1<t_2$或者$r_1<r_2$。$MQ'_{\mathrm{NET}}(q)$是消息集合$MS_{\mathrm{NET}}(q)$中的消息按$'\gtrsim'$降序排列后得到的序列。

下面归纳定义行动序列 Q 和参与者函数 p：

(1)空序列$\varnothing\in Q$, $p(\varnothing)=1$。

(2) 已知 $q\in Q$，$p(q)=v(v\in N^{'})$，则对任意 $a\in A_v(\Sigma_v(q))$ 有 $q.a\in Q$，如果 $P^{'}(q,v)\neq\varnothing$，则 $p(q.a)=k_{\min}(q.a,v)$；否则 $p(q.a)$= NET。

(3)已知 $q\in Q$, $p(q)$=NET，消息变量 m 的初始值是 $MQ^{'}_{\mathrm{NET}}(q)$ 的第一个消息，则：

1)如果 m 为空，则 $p(q)=k_{\min}(q,0)$，计数器加 1，进入下一轮；否则转 2)。

2)NET为 m 选取一个主动事件 $a\in A_{\mathrm{NET}}(\Sigma_{\mathrm{NET}}(q))$，则 $q.a\in Q$, $q=q.a$, $p(q)$=NET，m 被赋值为 $MQ^{'}_{\mathrm{NET}}(q)$ 的下一个消息，删除 $MQ^{'}_{\mathrm{NET}}(q)$ 的第一个消息；或者NET不选择任何事件，m 被赋值为 $MQ^{'}_{\mathrm{NET}}(q)$ 的下一个消息。

3)返回到 1)。

2.7 收益

收益是指在一个特定的战略组合下参与者得到的确定或期望的效用。假定博弈的 2 个极大行动序列 q_1 和 q_2，参与者 i 从 q_1 和 q_2 中获得的收益分别是 $u_i(q_1)$ 和 $u_i(q_2)$，则 $q_1\geqslant_i q_2$ 当且仅当 $u_i(q_1)\geqslant u_i(q_2)$。参与者的收益不仅取决于自己的策略选择，而且取决于所有参与者的策略选择。因此收益可以表示为所有参与者各选定一个策略形成的策略组合的函数。假设协议的交换项为 γ_i 和 $\gamma_j(i,j=1,2;\ i\neq j)$，实值 $r_i(\gamma_j)$ 表示参与者 i 拥有 γ_j 的控制权，实值 $r_i(\gamma_i)$ 表示 i 失去对 γ_i 的控制权，满足 $r_1(\gamma_2)>r_1(\gamma_1)>0$ 和 $r_2(\gamma_1)>r_2(\gamma_2)>0$。

定义 3 收益

$$u_i(q)=u_i^{+}(q)-u_i^{-}(q)$$

$$u_i^{+}(q)=\begin{cases} r_i(\gamma_j) & \phi_i^{+}(q)=\text{true}\\ 0 & \phi_i^{+}(q)=\text{false}\end{cases}$$

$$u_i^{-}(q)=\begin{cases} r_i(\gamma_i) & \phi_i^{-}(q)=\text{true}\\ 0 & \phi_i^{-}(q)=\text{false}\end{cases}$$

其中，i,j=1,2 且 $i\neq j$. $u_i^{+}(q)$ 表示参与者 i 的收入；$u_i^{-}(q)$ 表示 i 的支出；$u_i(q)$ 表示 i 的收益，是参与者收入和支出的差额。$\phi_i^{+}(q)$, $\phi_i^{-}(q)$ 是一阶逻辑公式。$\phi_i^{+}(q)$ 为真，当且仅当 i 拥有 γ_j，$\phi_i^{-}(q)$ 为真当且仅当 i 不是 γ_i 的唯一拥有者或者丢失 γ_i。由此可知 $u_i(q)=0$ 表示 i 的收入支出相抵，$u_i(q)>0$ 表示 i 获益，$u_i(q)<0$ 表示 i 的利益受到损害。由于TTP和NET不期望任何收益，因此假定对任何极大行动序列 q 满足 $u_{\mathrm{TTP}}(q)=u_{\mathrm{NET}}(q)=0$。

3 结束语

本文根据电子支付系统的分布并发式和动态博弈的特征，基于 CSP 相关理论和动态博弈理论建立了电子支付系统模型。该模型较好地刻画了参与者进程的交叠并发及其同步通信行为，以及各类主体之间的合作与竞争的关系，考虑了系统失效下协议的安全性质。该模型也可以对优化公平交换协议和公平非否认协议等电子商务协议建模，具有良好的扩展性。在后续的工作中将会进一步研究电子支付协议的自利性，使系统模型能更好地揭示电子支付的本质特征。

参考文献

[1] Zhou Jianying. Achieving Fair Non-repudiation in Electronic Transactions[J]. Journal of Organizational Computing and Electronic Commerce, 2001, 11(4): 253-267.

[2] Heintze N, Tygar J D, Wing J, et al. Model Checking Electronic Commerce Protocols[C]//Proc. of the 2nd USENIX Workshop on Electronic Commerce. Oakland, California, USA: [s. n.], 1996.

[3] Clarke E, Jha S, Marrero W. A Machine Checkable Logic of Knowledge for Specifying Security Properties of Electronic Commerce Protocols[C]//Proc. of the 13th IEEE Annual Symposium on Logic in Computer Science. Indianapolis, Indiana, USA: [s. n.], 1998.

[4] Kailar R. Reasoning About Accountability in Protocols for Electronic Commerce[C]//Proc. of the 14th IEEE Symposium on Security and Privacy. Atlanta, GA, USA: [s. n.], 1995.

[5] Hoare C A R. Communicating Sequential Processes[M]. [S. l.]: Prentice Hall, 2004.

[6] Osborne M, Rubinstein A. A Course in Game Theory[M]. [S. l.]: MIT Press, 1994.

(上接第 170 页)

表 1 基于 URPP 模型的安全加固操作系统测试结果

测试项目	测试手段	测试结果
进程合法性校验	运行不在合法进程范围内的进程	该进程无法启动，并提示在异常程序界面中
进程名称完整性校验	修改进程相关文件的名称	该进程不能正常启动，并提示在异常程序界面中
进程内容完整性校验	替换进程相关文件	该进程无法启动，并提示在异常程序界面中
防木马性能测试	投放 Rootkit 木马程序	该木马不能正常启动，并提示在异常程序界面中
防病毒性能测试	投放熊猫烧香病毒	被该病毒感染的进程均不能启动，并提示在异常程序界面中
进程访问权限控制	读取该进程没有读取权限的文件	操作被禁止
进程权限约束	修改系统文件	操作被禁止

5 结束语

本文针对当前访问控制模型无法对可执行恶意代码进行自我防御的现状，分析了基于角色的访问控制模型对防御可执行恶意代码的不足，提出了一个具有 4 个元素的 URPP 访问控制模型，描述了 URPP 模型中的元素映射和进程控制方法，并在此基础上探讨了 URPP 模型的扩展方法。通过支持 URPP 模型的安全操作系统的商用，证明了该模型能够有效地对可执行恶意代码进行自我防御。下一步将展开对 URPP 模型的研究，对大规模用户系统的应用场景进行分析，讨论 URPP 模型在此场景下的扩展问题。

参考文献

[1] 冯登国. 计算机通信网络安全[M]. 北京: 清华大学出版社, 2001.

[2] 李志英, 黄 强, 楼新远, 等. RBAC 模型研究、改进与实现[J]. 计算机应用, 2006, 26(l2): 2945-2947.

[3] Christensen S N, Fleury E, Sørensen K, et al. Process-based Access Control[EB/OL]. (2007-05-11). http://www.cs.aau.dk/~fleury/download/papers/pbac05.pdf.

[4] 梁金千, 管晓宏. 基于进程的访问控制模型[J]. 计算机工程, 2007, 33(2): 25-27.

[5] 余发江, 张焕国. 可信安全计算平台的一种实现[J]. 武汉大学学报: 理学版, 2004, 50(1): 69-73.