基于四方的安全电子商务支付协议分析与验证

肖仕成 李 开 甘早斌
(华中科技大学计算机学院 武汉 430074)

摘 要 以基于四方的安全电子商务支付协议为研究对象,建立了协议的有限状态模型以及安全计算树逻辑CTL公式,利用符号模型检测工具SMV对协议的原子性进行检测验证。验证结果证明,基于四方的安全电子商务支付协议满足电子支付的金钱原子性、商品原子性以及确认发送原子性,协议符合电子支付的原子性安全要求。

关键词 电子商务支付协议,模型检测,SMV,原子性
中图法分类号 TP309 **文献标识码** A

Analysis and Verification of Secure E-commerce Payment Protocol Based on Four Parties

XIAO Shi-cheng LI Kai GAN Zao-bin
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Both the finite state model and the CTL (Computation Tree Logic) formulations were first constructed for the secure e-commerce payment protocol based on four parties (FSET) in this paper. Then, the symbolic model checking (SMV) was used to analyze and verify the atomicity of the FSET protocol. The result of analysis and verification indicates that the FSET can meet with the money atomicity, the goods atomicity and the certified delivery, as well as the electronic payment security requirements.

Keywords E-commerce payment protocol, Model checking, SMV, Atomicity

1 引言

随着国际电子商务的迅速发展和普及,电子商务支付协议的原子性也越来越受到人们的重视[1]。1996年,Carnegie Mellon大学的J. D. Tygar教授第一次正式提出了电子支付的原子性概念[2],并提出了满足金钱原子性、商品原子性以及确认发送原子性的电子商务支付协议——Netbill协议[3]。但是该协议仅仅支持数字商品的电子支付,对于传统商品的电子商务支付却无能为力。而电子商务发展至今,建立能支持传统商品的、安全的、能确保金钱原子性、商品原子性和确认发送原子性的电子商务支付协议将是大势所趋。在此背景下,文献[4]提出了一个安全的、能确保电子商务支付的金钱原子性、商品原子性以及确认发送原子性的电子商务支付协议——基于四方的安全电子商务支付协议。

本文以基于四方的安全电子商务支付协议为研究对象,利用符号模型检测(Symbolic Model Checking)技术对其进行分析检测,给出协议的有限状态机模型以及协议的原子性安全CTL(Computation Tree Logic)公式,利用国际上流行的符号模型检测工具SMV对协议的原子性进行检测。

2 SMV符号模型检测

模型检验(Model Checking)是一种自动分析和验证技术,是形式化验证中很重要的一种方法,是一种面向有穷状态并发系统的验证技术[5]。目前,模型检测工具种类繁多,技术也越来越完善和成熟,如SPIN和符号模型检测工具SMV等。模型检测技术最初应用于硬件设计中,后来就慢慢应用于安全协议和软件的检验测试,并在安全协议的检测领域取得了不错的成就[6-8]。

SMV符号模型检测工具是美国卡耐基·梅隆大学的麦克米兰博士(L. McMillan)于1996年开发出来的模型检测工具软件[9]。SMV符号模型检测工具发展到今天,已成为了当前最流行的协议检测工具之一,成功验证检测了很多著名的通信协议,是一种非常实用的协议分析和验证检测工具[10,11]。SMV系统具有一套自己用来描述有限状态并发系统的规范语言。为了利用SMV系统分析检测协议系统,首先利用SMV的规范语言描述协议系统,即系统说明,再利用CTL(Computation Tree Logic)公式表示将要验证的协议系统的性质,即系统属性,然后把用SMV规范的语言描述的系统说明和系统属性提交给SMV系统运行检测。SMV系统接受输入后,先从系统规范中提取有序二叉决策图ODDB(Ordered Binary Decision Diagram)形式表示的迁移系统,再利用基于ODDB(Ordered Binary Decision Diagram)的搜索算法确定系统是否满足CTL公式表述的被检验的性质。若协

到稿日期:2011-03-30 返修日期:2011-06-03 本文受国家自然科学基金(70672041),湖北省自然科学基金(2007ABA307),中央高校基本科研业务费(2010MS112)资助。

肖仕成(1983—),男,硕士,主要研究领域为电子商务、网络安全;李 开(1968—),男,博士,讲师,主要研究领域为信任计算和电子商务,E-mail:likai@mail.hust.edu.cn(通信作者);甘早斌(1968—),男,博士,副教授,主要研究领域为电子商务、软件Agent技术及其支撑系统理论以及信任计算、软件代码安全。

议满足被检测的性质，则 SMV 系统给出 True 结论；若协议不满足被检测的性质，则 SMV 系统给出 False 结论并提供导致该结果的反例[9]。其工作原理如图 1 所示。

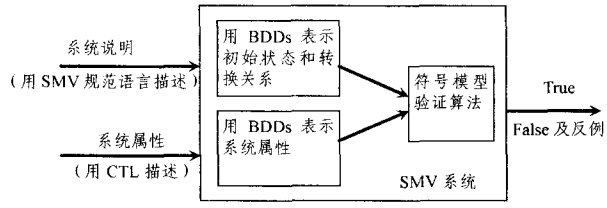

图 1　SMV 系统工作原理

3　基于四方的安全电子商务支付协议 SMV 分析建模

基于四方的安全电子商务支付协议由主协议、退货协议、换货协议以及交易欺诈纠纷处理协议组成[4]。对协议建模的交易主体包括客户 C、商家 M、支付机构 P 以及第四方 W。

3.1　基于四方的安全电子商务支付协议形式化模型描述

分析验证基于四方的安全电子商务支付协议的原子性，为方便描述，暂忽视协议的加解密过程，重点研究协议的资金流和物流的转移。下面描述基于四方的安全电子商务支付协议的消息。

3.1.1　基于四方的安全电子商务支付协议的主协议消息描述

基于四方的安全电子商务支付协议的主协议是协议的核心部分，其消息传递过程简单描述如下。

$Msg1$　$C\rightarrow M$：客户浏览商家商品并向商家发送订单信息；

$Msg2$　$M\rightarrow C$：商家生成双方都承认的、防篡改的电子证据文件及支付要求，发送给客户；

$Msg3$　$C\rightarrow P$：客户把支付指令和该交易的电子证据发送给支付机构；

$Msg4$　$P\rightarrow M\&W$：支付机构把交易可完成的消息分别发送给商家和第四方，第四方记录该交易，商家发货；

$Msg5$　$W\rightarrow P\&P\rightarrow C$：第四方把商家已发货信息发送给支付机构，支付机构再把该信息发送给客户；

$Msg6$　$W\rightarrow P\&P\rightarrow M$：第四方把客户已签单信息发送给支付机构，支付机构再把该信息发送给商家。

主协议结束后，启动计时器 T。如果客户满意本次交易，支付协议成功结束；如果客户对本次交易不满，设定客户在某一定时间参数 T 内，根据需要选择执行换货协议、退货协议或者交易欺诈纠纷处理协议。为方便描述，设置跳转参数 N，控制协议跳转到换货协议（$N=2$）或退货协议（$N=3$）或者交易欺诈纠纷处理协议（$N=4$）。在交易欺诈纠纷处理协议中，为区分客户和商家欺诈，设置参数 Q，若 $Q=1$，客户欺诈；$Q=2$，商家欺诈。

3.1.2　基于四方的安全电子商务支付协议的换货协议消息描述

若主协议执行完毕后商品存在质量问题，客户可选择执行换货协议。为防止协议进行换货时出现协议死循环，只允许客户执行一次换货协议，故设定一参数 R。协议初始化时，初始化 $R=1$；当执行 1 次换货协议时，令 $R=0$。当主协议结束时，客户申请执行退货协议，检测参数 R，选择执行换货协议。

基于四方的安全电子商务支付协议的换货协议消息描述如下。

$Msg7$　$C\rightarrow P$：客户发送换货申请信息给支付机构；

$Msg8$　$P\rightarrow C\&W$：支付机构把客户换货信息发送给客户和第四方；

$Msg9$　$W\rightarrow P\&P\rightarrow M$：第四方把客户换货已退货信息发送给支付机构，支付机构再把该信息发送给商家；

$Msg5$　$W\rightarrow P\&P\rightarrow C$：商家收到客户退货商品后，自动跳转到主协议，发送 $Msg5$ 步骤。

3.1.3　基于四方的安全电子商务支付协议的退货协议消息描述

基于四方的安全电子商务支付协议的主协议执行完毕以后，客户若对商品不满意，可选择执行退货协议。基于四方的安全电子商务支付协议的退货协议消息描述如下。

$Msg7'$　$C\rightarrow P$：客户发送退货的信息给支付机构；

$Msg8'$　$P\rightarrow C\&W$：支付机构把要求客户退货和信息发送给客户和第四方；

$Msg9'$　$W\rightarrow P\&P\rightarrow M$：第四方把客户已退货信息发送给支付机构，支付机构再把该信息发送给商家，交易结束。

3.1.4　基于四方的安全电子商务支付协议的纠纷处理协议消息描述

客户若发现所购商品与订单信息不符，可进行申请纠纷处理，执行交易欺诈纠纷处理协议。基于四方的安全电子商务支付协议的交易欺诈纠纷处理协议消息描述如下。

$Msg7''$　$C\rightarrow P$：客户发送纠纷处理申请信息给支付机构；

$Msg8''$　$P\rightarrow W$：支付机构把电子证据文件发送给第四方；

$Msg9''$　$(W\rightarrow P)\&[(P\rightarrow C)\ \text{or}\ (P\rightarrow M)]$：第四方把纠纷处理结果信息发送给支付机构，为方便描述，设置参数，以分辨客户或者商家欺诈，控制状态变换走向，如果是客户欺诈，支付机构把该信息转发给客户并对客户进行相关处罚，交易结束；如果是商家欺诈，支付机构把该信息转发给商家，并对商家进行相关处罚；

$Msg8'$　$P\rightarrow C\&W$：支付机构把要求客户退货的信息发送给客户和第四方，即跳转到退货协议的 $Msg8'$ 步骤。

3.2　基于四方的安全电子商务支付协议的有限状态模型

基于四方的安全电子商务支付协议的参与实体为：客户 C、商家 M、支付机构 P 和第四方 W，每个参与主体都在 SMV 系统中分别对应一个有限状态转换系统。

为方便描述，先对其符号进行定义，如表 1 所列。

表 1　符号定义描述

符号	含义	符号	含义
idle	空闲状态	! Msgn	主体发送消息 Msgn
? Msgn	主体接收消息 Msgn	ε	主体自动进入某一状态
X-G-Msgn	主体 X 生成消息 Msgn	X-W-Msgn	表示主体 X 等待消息 Msgn
X-Success	主体 X 成功完成一次协议	P-Cmon	参数，初始值为 0，当支付机构 P 把客户 C 的付款划拨到临时账户，赋值为 1
P-Credit	参数，初始值为 0，当支付机构支付机构 P 把客户 C 的付款从临时账号里划拨到商家 M 的账户时，赋值为 1	P-Amon	参数，初始值为 0，当支付机构 P 把客户 C 的付款从临时账号里划拨回客户 C 的账户时，赋值为 1

3.2.1 客户 C 的有限状态模型

模拟协议运行过程，对客户 C 建立有限状态机模型。客户 C 的状态包括 *idle*，*C-G-Msg*1，*C-W-Msg*2，*C-G-Msg*3，*C-W-Msg*5，*C-G-Msg*7，*C-W-Msg*8，*C-G-Msg*7′，*C-W-Msg*8′，*C-G-Msg*7″，*C-W-Msg*9″，*C-Success*。其中客户 C 的交易初始状态为 *C-G-Msg*1，交易结束状态为 *C-Success*。客户 C 的有限状态转换图如图 2 所示。

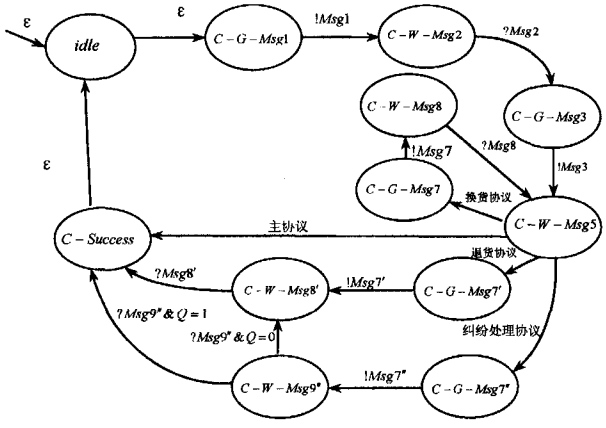

图 2 客户 C 的有限状态转换图

交易开始之前，客户 C 处于 *idle* 空闲状态。客户在网上浏览购买商品时，自动进入 *C-G-Msg*1 状态，发送消息 *Msg*1 后，进入 *C-W-Msg*2 状态。客户等待并接收到符合协议格式的消息 *Msg*2 后，进入 *C-G-Msg*3 状态，生成消息 *Msg*3 后，进入状态 *C-W-Msg*5。当收到与协议格式相符的消息 *Msg*5 后，客户 C 准备收货。客户收到货物后，根据需要在申诉时间 T 内选择运行换货协议、退货协议和交易欺诈处理协议等。

客户如果对商品满意，且在申诉时间 T 内没有向支付机构 P 申诉，即 $T=0$，则直接进入 *C-Success* 状态，完成一次交易。

客户若在申诉时间 T 内向支付机构 P 进行申诉，$N=2$，检查换货参数 R，检测换货协议条件，即 $T!=0\&N=2\&R=1$，则进入 *C-G-Msg*7 状态，生成并发送消息 *Msg*7，进入 *C-W-Msg*8 状态，等待并接收到符合协议格式的消息 *Msg*8 后，进入 *C-W-Msg*5 状态。

客户若在申诉时间 T 内申请退货，即 $T!=0\&N=3$，则进入 *C-G-Msg*7′状态，生成并发送消息 *Msg*7′，进入状态 *C-W-Msg*8′，接收到符合协议格式的消息 *Msg*8′后，进入 *C-Success*，完成一次交易。

客户在申诉时间 T 内向支付机构 P 进行交易纠纷处理，即 $T!=0\&N=4$，进入 *C-G-Msg*7″状态，生成并发送 *Msg*7″消息，进入 *C-W-Msg*9″状态，并等待符合协议格式的 *Msg*9″消息。客户收到 *Msg*9″消息后，检查消息内容，若为客户欺诈消息，即 $Q=1$，直接进入 *C-Success* 状态，若为商家欺诈，即 $Q=2$，进入 *C-W-Msg*8′状态。客户接收到符合协议格式的消息 *Msg*8′后，进入 *C-Success* 状态，完成一次交易。

3.2.2 商家 M 的有限状态模型

模拟协议运行过程，为商家 M 建立有限状态机模型。商家 M 的状态包括 *idle*，*M-W-Msg*1，*M-G-Msg*2，*M-W-Msg*4，*M-W-Msg*6，*M-W-Msg*9，*M-W-Msg*9′，*M-W-Msg*9″，*M-Success*。其中商家 M 的交易初始状态为 *M-W-Msg*1，交易结束状态为 *M-Success*。商家 M 的有限状态转换图如图 3 所示。

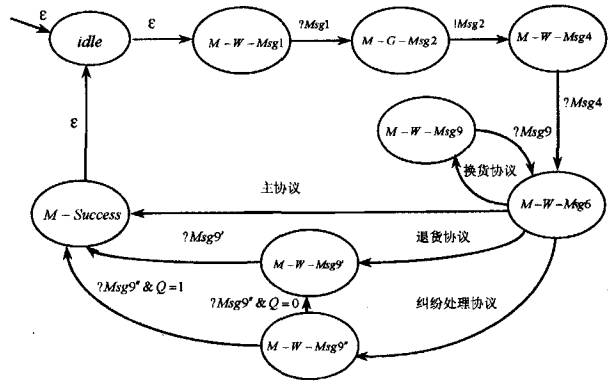

图 3 商家 M 的有限状态转换图

商家 M 直接从空闲状态 *idle* 进入 *M-W-Msg*1 状态，收到符合协议格式的消息 *Msg*1 后，进入 *M-G-Msg*2 状态，生成并发送 *Msg*2 消息，进入 *M-W-Msg*4 状态，收到符合协议格式的 *Msg*4 消息后，直接进入 *M-W-Msg*6 状态，收到符合协议格式的 *Msg*6 消息后，等待交易申诉。

若 $T=0$，直接进入 *M-Success* 状态，完成一次交易。

若 $T!=0\&N=2$，进入 *M-W-Msg*9，收到协议格式的 *Msg*9 消息后，回到 *M-W-Msg*6 状态。

若 $T!=0\&N=3$，进入 *M-W-Msg*9′状态，收到符合协议格式的 *Msg*9′后，进入 *M-Success* 状态，完成一次交易。

若 $T!=0\&N=4$，进入 *M-W-Msg*9″，收到协议格式的 *Msg*9″消息后，若 $Q=1$，进入 *M-Success* 状态，完成一次交易；若 $Q=2$，进入 *M-W-Msg*9′状态，收到符合协议格式的 *Msg*9′后，进入 *M-Success* 状态，完成交易。

3.2.3 支付机构 P 的有限状态模型

模拟协议运行过程，为支付机构 P 建立有限状态机模型。支付机构 P 的状态包括 *idle*，*P-W-Msg*3，*P-G-Msg*4，*P-W-Msg*5，*P-G-Msg*5，*P-W-Msg*6，*P-G-Msg*6，*P-W-Msg*7，*P-G-Msg*8，*P-W-Msg*9，*P-G-Msg*9，*P-W-Msg*7′，*P-G-Msg*8′，*P-W-Msg*9′，*P-G-Msg*9′，*P-W-Msg*7″，*P-G-Msg*8″，*P-W-Msg*9″，*P-G-Msg*9″，*P-Success*。其中支付机构 P 的交易初始状态为 *P-W-Msg*3，交易结束状态为 *P-Success*。支付机构 P 的有限状态转换图如图 4 所示。

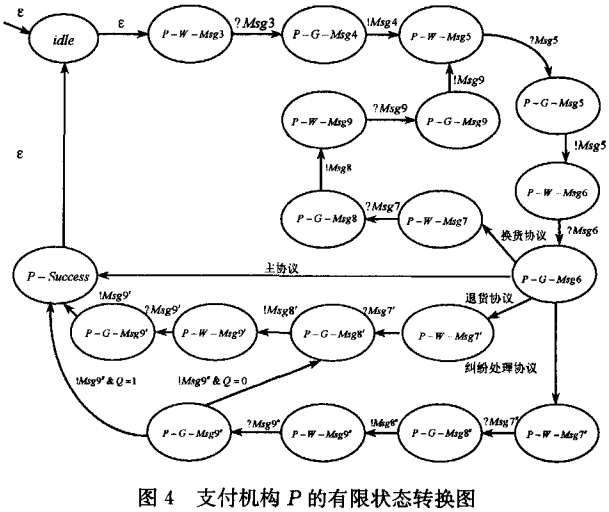

图 4 支付机构 P 的有限状态转换图

支付机构 P 直接从 *idle* 状态进入 *P-W-Msg*3 状态，收到符合协议格式的 *Msg*3 信息后，把客户付款暂时划拨到临时账户，即 *P-Cmon*=1，再进入 *P-G-Msg*4 状态，生成发送 *Msg*4

信息后，进入 *P-W-Msg*5 状态，收到符合协议格式的 *Msg*5 信息后，进入 *P-G-Msg*5 状态，即转发 *Msg*5 信息，进入 *P-W-Msg*6 状态，收到符合协议格式的 *Msg*6 信息后，进入 *P-G-Msg*6 状态，即转发 *Msg*6 信息，启动计时参数 *T*，等待客户申诉。

若 *T*! =0&*N*=2&*R*=1，进入 *P-W-Msg*7 状态，收到符合协议格式的 *Msg*7 消息后，进入 *P-G-Msg*8 状态，生成发送 *Msg*8 消息后，进入 *P-W-Msg*9 状态，收到符合协议格式的 *Msg*9 消息后，进入 *P-G-Msg*9 状态，即转发 *Msg*9 消息，回到 *P-W-Msg*5 状态。

若 *T*=0，令 *P-Credit*=1，即往商家账户转账，自动进入 *P-Success* 状态，完成一次交易。

若 *T*! =0&*N*=3，进入 *P-W-Msg*7′状态，收到符合协议格式的 *Msg*7′消息后，进入 *P-G-Msg*8′状态，生成发送 *Msg*8′消息，进入 *P-W-Msg*9′状态，收到符合协议格式的 *Msg*9′消息后，进入 *P-G-Msg*9′状态，即转发 *Msg*9′消息，令 *P-Amon*=1，即把临时账户里的钱划拨回客户的账户里，进入 *P-Success* 状态，完成一次交易。

若 *T*! =0&*N*=4，进入 *P-W-Msg*7″状态，收到符合协议格式的 *Msg*7″消息后，进入到 *P-G-Msg*8″状态，生成并发送 *Msg*8″消息，进入 *P-W-Msg*9″状态，收到符合协议格式的 *Msg*9″消息后，进入 *P-G-Msg*9″状态，即转发 *Msg*9″消息，检查参数 *Q*，若 *Q*=2，回到 *P-G-Msg*8′状态，若 *Q*=1，令 *P-Credit*=1，即把临时账户里的钱划拨到商家的账户里，进入 *P-Success* 状态，完成一次交易。

3.2.4 第四方 *W* 的有限状态模型

模拟协议运行过程，为第四方 *W* 建立有限状态机模型。第四方 *W* 的状态包括 *idle*，*W-W-Msg*4，*W-G-Msg*5，*W-G-Msg*6，*W-W-Msg*8，*W-G-Msg*9，*W-W-Msg*8′，*W-G-Msg*9′，*W-W-Msg*8″，*W-G-Msg*9″，*W-Success*。其中第四方 *W* 的交易初始状态为 *W-W-Msg*4，交易结束状态为 *W-Success*。第四方 *W* 的有限状态转换图如图 5 所示。

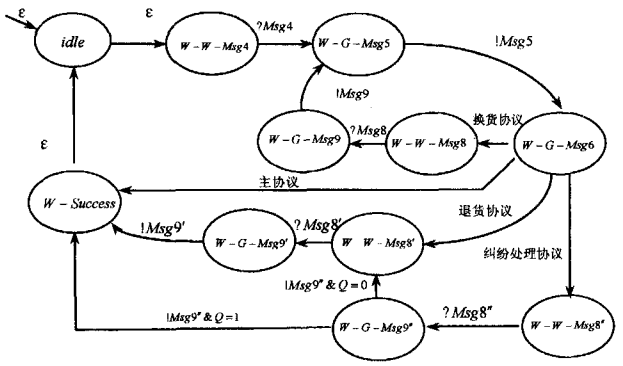

图 5 第四方 *W* 的有限状态转换图

第四方 *W* 从 *idle* 空闲状态直接进入 *W-W-Msg*4 状态，收到符合协议格式的 *Msg*4 后，接收商家发货，进入 *W-G-Msg*5 状态，生成发送 *Msg*5 消息后，进入 *W-G-Msg*6 状态，生成发送 *Msg*6 消息后，等待交易申诉。

若 *T*! =0&*N*=2，进入 *W-W-Msg*8 状态，收到符合协议格式的 *Msg*8 后，进入 *W-G-Msg*9 状态，生成发送 *Msg*9 消息，回到 *W-G-Msg*5 状态。

若 *T*=0，直接进入 *W-Success* 状态，完成一次交易。

若 *T*! =0&*N*=3，进入 *W-W-Msg*8′状态，收到符合协议格式的 *Msg*8′消息后，进入 *W-G-Msg*9′状态，生成发送 *Msg*9′消息，进入 *W-Success* 状态，完成一次交易。

若 *T*! =0&*N*=4，进入 *W-W-Msg*8″状态，收到符合协议格式的 *Msg*8″消息后，进入 *W-G-Msg*9″状态，生成发送 *Msg*9″消息，检测参数 *Q*，若 *Q*=2，回到 *W-W-Msg*8′状态，若 *Q*=1，进入 *W-Success* 状态，完成一次交易。

4 基于四方的安全电子商务支付协议的 CTL 原子性属性描述

4.1 金钱原子性(Money Atomicity)

金钱原子性指的是在电子商务交易活动中，金钱不会凭空产生，也不会凭空消失，而且客户支付的金钱金额数等于商家得到的金钱金额数。也就是说在电子交易中，当且仅当客户 *C* 支付了货款，商家 *M* 才能得到货款。CTL 公式描述如 R1、R2。

R1：$AG((P-Cmon=1)\&(\sim EF(PAmon=1)))->AF(P-Credit=1)$

R2：$\sim E((P-Cmon=0)U(P-Credit=1))$

4.2 商品原子性(Goods Atomicity)

商品原子性指的是在电子商务交易活动中，当且仅当客户收到商品并确认无误之后，商家才能收到货款。CTL 公式描述如 R3、R4。

R3：$AG(P-Credit=1)->AF(P.State=P-G-Msg6)$

R4：$AG((P.State=P-G-Msg6)\&(\sim EF(P-Amon=1)))->AF(P-Credit=1)$

4.3 确认发送原子性(Certified Delivery Atomicity)

确认发送原子性指的是在电子商务交易活动中，商家发送给客户的商品确实为客户订购的商品。由于协议牵涉到复杂的加解密运算，故要求每次交易中仲裁机构都能收到商家和客户对商品不可否认的电子证据文件。CTL 公式描述如 R5。

R5：$\sim E((\sim E(P.State=P-W-Msg3))U((P.State=P-Success)\&(C.State=C-Success)))$

5 基于四方的安全电子商务支付协议模型检测验证结论

由于 SMV 语言是描述并发的语言，故可以用 SMV 程序并发执行协议参与方并发进程，模拟整个安全协议的信息交互和处理全过程。基于四方的安全电子商务支付协议交易参与方为客户、商家、支付机构以及第四方，故可分为 4 个模块。再定义一个公共信息模块，用以保存 4 个交易模块的公共交互信息。4 个模块模拟协议运行的信息交互全过程。

利用基于四方的安全电子商务支付协议 SMV 有限状态模型，将其转换成 SMV 程序，模拟整个协议运行过程。为便于实验观察，分别对基于四方的安全电子商务支付协议的主协议、退货协议、换货协议以及交易欺诈纠纷处理协议进行原子性安全检测测试。将 SMV 程序和其必须满足的 CTL 公式 R1、R2、R3、R4、R5 输入到 SMV 检测工具中运行，得到的结论均为 True，运行检测结果如图 6 所示。由此可知基于四方的安全电子商务支付协议满足上述的原子性属性，即基于

(下转第 92 页)

18(4):460-473

[8] Spitz S, Tuchelmann Y. A Trust Model Considering the Aspects of Time[C]// Proceedings of the Second International Conference on Computer and Electrical Engineering(ICCEE). USA: IEEE Computer Soc, 2009:550-554

[9] Srivatsa M, Liu L. Vulnerabilities and security issues in structured overlay networks: A quantitative analysis[C]// Proceedings of the 20th Annual Computer Security Applications Conference(ACSAC). USA: IEEE Computer Society, 2004:252-261

[10] 李勇军,代亚非. 对等网络信任机制研究[J]. 计算机学报,2010,33:390-405

[11] Yuh-Min T, Fu-Gui C. A free-rider aware reputation system for peer-to-peer file-sharing networks[J]. Expert Systems with Applications, 2011, 38(3):2432-2440

[12] 余一娇,金海. 对等网络中的搭便车行为分析与抑制机制综述[J]. 计算机学报,2008,31(1):1-15

[13] 常俊胜,王怀民,尹刚. DyTrust:一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报,2006,29(8):1301-1307

[14] Karakaya M, Korpeoglu I O. Free riding in Peer-to-Peer Networks[J]. IEEE Internet Computing, 2009, 13(2):92-98

[15] Query Cycle Simulator [EB/OL]. http://p2p.stanford.edu/www/qcsim.htm

[16] Schlosser M, Condie T, Kamvar S. Simulating a File-Sharing P2P Network[C]// Proceedings of the 1st Workshop on Semantics in Grid and P2P Networks. USA: Stanford Inforlab Publication Server, 2003

[17] 胡建理,吴泉源,周斌. P2P 环境下基于信誉的信任模型研究[J]. 计算机科学,2009,36(9):1-6

(上接第 78 页)

四方的安全电子商务支付协议满足金钱原子性、商品原子性以及确认发送原子性。

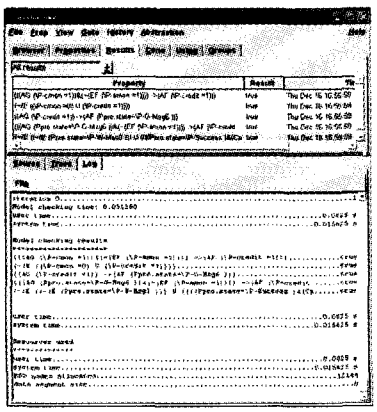

图 6 基于四方的安全电子商务支付协议实验检测结果

本次实验利用符号模型检测工具 SMV 对基于四方的安全电子商务支付协议进行原子性安全检测,证明了协议具备电子支付原子性安全需求,存在很大的实际意义。基于四方的安全电子商务支付协议首次实现传统商品在电子商务支付活动中的原子性。而据调查显示,人们在网络购物活动中,支付后收不到商品、假货的存在以及退换货的不便是影响网民网上购物热情的重要因素。而基于四方的安全电子商务支付协议解决了电子商务支付安全的原子性问题,彻底改变了客户在电子商务退换货活动中的被动地位,让退换货的主动权掌握在客户手中,这将对电子商务的普及和发展起着巨大的作用。

结束语 根据基于四方的安全电子商务支付协议模型,利用 SMV 工具从协议的原子性方面对协议进行了验证,证明了基于四方的安全电子商务支付协议符合电子商务的原子性要求,确保了电子商务活动中电子支付的金钱原子性、商品原子性以及确认发送原子性,保证了电子支付的安全,很好地满足了传统实物商品的原子性要求,这将对电子商务的发展起到一定的推动作用。

参 考 文 献

[1] 刘义春,张焕国,王丽娜. 电子支付协议的原子性研究综述[J]. 计算机科学,2005,32(2):93-96,113

[2] Tygae J D. Atomicity in electronic commerce[C]// Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing. May 1996:8-26

[3] Cox B, Tygar J D. NetBill security and transaction protocol[C]// Proceedings of the 1st USENIX Workshop on Electronic Commerce. July 1995:77-88

[4] 甘早斌,肖仕成. 基于四方的安全电子商务支付协议研究[J]. 计算机科学,2011(10)

[5] 薛锐,冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报,2006,29(1):1-20

[6] Lu Shi-yong, Smolka S A. Model Checking the Secure Electronic Transaction (SET) protocol[C]// Proceedings of the 7th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems. 1999:358-365

[7] Lu Si-mei, Zhang Jian-lin, Luo Li-ming. The automatic verification and improvement of SET protocol model with SMV[C]// Proceedings of the International Symposium on Information Engineering and Electronic Commerce(IEEC '09). Ternopil, May 2009:433-436

[8] Talukder K H, Harada K. Modeling and verification of some communication protocols[C]// Proceedings of the 8th International Conference, Advanced Communication Technology (ICACT 2006). Phoenix Park, February 2006:2193-2198

[9] McMillan L. Symbolic Model Checking[M]. Pittsburgh, USAL: Kluwer Academic Publisher, 1993

[10] Liu Xia, Huang Qi, Chen Yong. Model Checking of Wireless Transaction Protocol[C]// Proceedings of 2009 World Congress on Computer Science and Information Engineering. 2009: 620-623

[11] Ning Ning, Zhang Jun, Gao Xiang-yang. Formal Verification of SDG via Symbolic Model Checking[C]// Proceedings of Second International Conference on Intelligent Computation Technology and Automation(ICICTA '09). October 2009:521-524