一种新的电子商务协议分析方法

郭 华[1] 李舟军[1] 庄 雷[2] 计宏霖[3]
(北京航空航天大学计算机学院 北京 100083)[1] (郑州大学信息工程学院 郑州 450052)[2]
(信息工程大学信息工程学院 郑州 450002)[3]

摘 要 基于卿-周逻辑给出了一些新的逻辑推理规则,并提出了一种扩展的通信有限状态自动机,用于分析电子商务协议的安全性质。该方法可描述协议参与者的行为与知识,且无需人为地引入初始假设。对扩展模型抽象并修改后,还可验证其它一些与加密、签名消息无关的性质。利用该方法分析了匿名可恢复的公平交换协议,发现其满足有效性、公平性、可追究性,但不满足匿名性,并用 UPPAAL 验证了协议的公平性、活性与时效性等。

关键词 电子商务协议,模型检测,逻辑分析,通信有限状态自动机
中图法分类号 TP309 **文献标识码** A

New Approach for Analyzing of E-commerce Protocol

GUO Hua[1] LI Zhou-jun[1] ZHUANG Lei[2] JI Hong-lin[3]
(School of Computer Science and Engineering, Beihang University, Beijing 100083, China)[1]
(Institute of Information Engineering, Zhengzhou University, Zhengzhou 450052, China)[2]
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)[3]

Abstract This paper presented an extended CSFM by combining communication finite state machine (CSFM) with some new logic rules based on Qing-Zhou logic to analyze security properties of E-commerce protocols. It not only can describe the knowledge and behavior of participants, but also analyze the security properties without initial state assumptions. In addition, this method enables us to verity other security properties after abstracting and modifying the model. Using this method, accountability, fairness and atomicity were analyzed to be satisfied in the anonymous and failure resilient fair-exchange ecommerce protocol. Then UPPAAL was used to verify the properties of fairness, liveness and timeliness.

Keywords E-commerce protocol, Model checking, Logic proving, Communication finite state machine

1 引言

电子商务协议的基本属性包括有效性、可追究性、公平性、匿名性、时效性等。对电子商务协议形式化建模并分析,得到的结果可用于指导设计协议或弥补原协议中的缺陷。因此,研究电子商务协议的形式化分析方法及其相应的支持工具,具有重要的理论意义和应用价值。

模型检测是一种常见的分析协议的形式化方法。它直观明了,可借助模型检测工具实现自动验证。自 1996 年 Lowe[1] 首先应用 CSP 理论和模型校验工具 FDR 分析 NSPK 协议并发现一个近 17 年未知的攻击之后,使用模型检测理论及相对应的支持工具分析电子商务协议成为一个热点[2-4]。但模型检测的方法不具备逻辑推理能力,因此无法分析可追究性、公平性、匿名性等一些特殊的安全性质。

基于逻辑的方法是近几年来一种重要的电子商务协议形式化分析方法[5-11]。Kailar[5] 逻辑可分析协议的可追究性,但无法分析公平性;卿斯汉[6,7] 等提出了卿-周逻辑用于分析可追究性和公平性。文献[8]用基于博弈的 ATL(alternating-time temporal logic)逻辑描述协议的常见性质,并用模型检测工具 MOCHA 分析了公平性、时效性等,将 Kailar 逻辑和 LPC(logic process calculus)方法结合[9],可分析协议的公平性和可追究性。但基于逻辑的方法不能明确表示协议参与者的行为,且不能分析协议的死锁、活锁等安全性质。

基于在线第三方的公平交换协议是针对电子商务环境中顾客和商家互不信任的问题而提出的:第三方从顾客和商家接收到要交换的物品,然后以一种公平的方式转发给对方,但第三方很容易成为协议的瓶颈。2005 年,Ray[12] 等人提出了一个匿名可恢复的公平交换协议(anonymous and failure resilient fair-exchange ecommerce protocol, AFRFE)。在该协议中,可信第三方只在参与者作弊或出现通信故障时才参与

到稿日期:2009-09-05 返修日期:2009-12-11 本文受国家自然科学基金项目(60473057,60973105),北京航空航天大学博士生创新基金(211619)资助。

郭 华(1980—),女,博士生,主要研究方向为信息安全,E-mail:guohua80125@sina.com;李舟军(1963—),男,博士,教授,CCF 会员,主要研究方向为信息安全;庄 雷(1963—),女,博士,教授,CCF 会员,主要研究方向为协议验证;计宏霖(1973—),男,硕士生,主要研究方向为协议验证。

协议，并可在协议范围内自动解决争端。但作者只是启发式地分析了协议的一些安全性质，如有效接收性、货币原子性和公平性等。目前尚未有形式化分析该协议的工作。

本文将卿-周逻辑引入通信有限状态自动机(communication finite state machine，CSFM)[13]来形式化分析 AFRFE 协议。首先将逻辑引入 CSFM，提出一个扩展的自动机模型：自动机的状态集扩展为知识集和公式集组成的二元组，利用消息及逻辑转换规则确定状态的转换。之后对模型抽象并修改，用时间自动机为协议建模，并借助自动验证工具 UPPAAL[14]分析了协议的活性和时效性。

2 将逻辑引入 CSFM 的形式化分析方法

2.1 推理规则

首先基于卿-周逻辑给出一些推理规则。基本符号的表示方法与卿-周逻辑[6,7]相同。

R1 签名规则：$\dfrac{P \ni \{x\}_{k_q^{-1}} P \xrightarrow{k_q} Q}{P \succ Q \rightarrow x}$

若 P 拥有用 k_q^{-1} 签名的消息 x，并且 P 能证明 k_q 可用于验证 Q 的身份，则 P 可证明 Q 对 x 负有责任。

R2 密文理解规则：$\dfrac{P \succ Q \rightarrow \{x\}_k, P \succ Q \ni k}{P \succ Q \rightarrow x}$

若 P 能证明 Q 对某个用密钥 k 加密的消息 x 负责，并且 P 能证明 Q 拥有加密密钥 k，那么 P 能证明 Q 对 x 负责。

R3 密文拥有规则：$\dfrac{P \ni \{x\}_k, P \ni k}{P \ni x}$

如果 P 收到某个用密钥 k 加密的消息 x，并且 P 拥有加密密钥 k，那么 P 拥有 x。

R4 签名拥有规则：$\dfrac{P \ni \{x\}_{k_q^{-1}}}{P \ni x}$

假设 P 收到了用 k_q^{-1} 签名的消息 x，则 P 一定拥有 x。

R5 消息认证规则：$\dfrac{P \succ Q \rightarrow CC(x)}{P \succ Q \rightarrow x}$

若 P 能证明 Q 对某个消息认证码 $CC(x)$ 负责，则 P 能证明 Q 对消息 x 负责。

R6 身份认证规则：$\dfrac{P \succ Q \rightarrow x}{P \in ID(Q)}$

若 P 能证明 Q 对 x 负责，则 P 知道 Q 的身份。

R7 传递规则：$\dfrac{P \succ Q \rightarrow x, Q \succ R \rightarrow x}{P \succ R \rightarrow x}$

如果 P 能证明 Q 对 x 负责且 Q 能证明 R 对 x 负责，则 P 能证明 R 对 x 负责。

其中，R4－R7 是新引入的规则，用于分析可追究性、公平性及匿名性等。

下面介绍扩展的自动机模型。

定义 1 具有逻辑推理能力的通信有限状态自动机(LCFSM)是一个八元组：$L=(S,N,K,F,MA,R,\delta,S_{Initial})$，其中：

(1)S 为有限状态集，状态 $s_i \in S$ 是一个二元组$(S_i,(K_i,F_i))$，其中 S_i 是 s_i 的标号；$K_i \subseteq K$ 为知识集，记录了当前状态下参与者拥有的知识；$F_i \subseteq F$ 为公式集，记录了当前状态下参与者拥有的公式；

(2)N 是协议所有参与者的名字集；

(3)K 为知识集，由参与者自身拥有的初始知识、协议执行过程中发送或接收的消息及这些消息的组合知识组成，随协议执行变化；

(4)F 为公式集，由参与者自身拥有的初始公式、协议执行过程中从已有公式用推理规则推出的新公式组成，随协议执行变化；

(5)MA 为消息动作集，即 $MA=\{m!$ 或 $m?\mid m \in M\}$；

(6)R 为推理规则集，由上述的推理规则组成；

(7)δ 是状态转移函数，$\delta: S \times (M \cup R) \rightarrow S$；

(8)$S_{Initial} \subseteq S$，表示初始状态集。

LCFSM 的状态转换由状态转移函数 δ 定义，状态转换有两种类型：a)由接收或发送消息的动作触发的状态转换；b)由推理规则触发的状态转换。

定义 2 LCFSM 的状态是一个二元组$(S_i,(K_i,F_i))$，状态转换规则如下：

a)状态随消息而转换；

(1)对一个状态$(S_i,(K_i,F_i))$及发送消息 $m!$，有$(S_i,(K_i,F_i)) \xrightarrow{m!} (S_j,(K_j,F_j))$。转换发生后，状态标志符由 S_i 变为 S_j，公式集不变，知识集按如下规则改变：

若 $m \in K_i$，则知识集不变，即 $K_j=K_i$；

若 $m \notin K_i$，设 $m=(m_1,m_2,\cdots)$，其中 $k_1 \in K_i, k_2 \in K_i, m_1 \notin K_i, m_2 \notin K_i$，且 m_1、m_2 分别为知识 m_1'、m_2'在密钥 k_1、k_2 下的加密、签名或认证消息，即 m 由若干个不在 K_i 中出现的消息 m_1、m_2 及其它消息复合而成，则 $K_j=K_i \cup \{m,m_1,m_2\}$。

(2)对一个状态$(S_i,(K_i,F_i))$及接收消息 $m?$，有$(S_i,(K_i,F_i)) \xrightarrow{m?} (S_j,(K_j,F_j))$。转换发生后，状态标志符由 S_i 变为 S_j，公式集不变。设 $m=(m_1,m_2,\cdots)$，则 $K_j=K_i \cup \{m,m_1,m_2,\cdots\}$。

(3)检查转换后的公式集 F_j，若有 $P \ni m$ 且 $m \notin K_i$，则 $K_j=K_i \cup \{m\}$。

b)状态随推理规则而转换；

对一个状态$(S_i,(K_i,F_i))$及一个推理规则 r，有$(S_i,(K_i,F_i)) \xrightarrow{r} (S_j,(K_j,F_j))$。转换发生后，状态标志符由 S_i 变为 S_j，知识集不变。公式集按推理规则改变，即假设 r 为形如$\dfrac{A;B}{C}$的推理规则，其中 $A,B \in F_i$，则转换发生后，$F_j = F_i \cup \{C\}$。此外，若 $m \in K_j$ 且 $P \ni m \notin F_i$，则 $F_j = F_i \cup \{P \ni m\}$。

在状态随推理规则转换的过程中，由于知识集不变，将形如$(S_i,(K_i,F_i)) \xrightarrow{r_1} (S_j,(K_j,F_j)) \xrightarrow{r_2} (S_k,(K_k,F_k))$简记为$(S_i,(K_i,F_i)) \xrightarrow{r_1,r_2} (S_k,(K_k,F_k))$。

3 实例分析

假设通信信道是安全的，协议所采用的密码算法是“完善”的且 TTP 和一般主体之间的通信信道是可恢复的。本节以 AFRFE 协议为例，用 LCFSM 为协议建模并分析安全性质。

3.1 协议描述

AFRFE 协议由基本协议和扩展协议两部分组成。协议中的基本符号描述见文献[12]，此处给出简单的协议描述。

基本协议：

(1)$TP \rightarrow C: [m,k_M]$；

(2)$C \rightarrow M: PO, [CC(PO), C_{prv}], [[PT, k_{C_1} \times k_{C_2}], B_{prv}], B$；

(3)M→C:[[CC(PO),C_{prv}],M_{prv}],[mr,$k_M\times k_{M_1}$],[r,k_{M_1}],[[CC([r,k_{M_1}]),M_{prv}],[[CC([mr,$k_M\times k_{M_1}$]),M_{prv}]; or M→C:Abort;

(4)C→M:[$k_{C_2}^{-1}$,M_{pub}],[[CC([m,$k_M\times k_{M_1}$]),C_{prv}]; or C→M:Abort,[[CC([m,$k_M\times k_{M_1}$]),C_{prv}];

(5)M→C:[$k_{M_1}^{-1}$,C_{pub}],[r^{-1},C_{pub}]。

扩展协议:

(1)C→TP:M,[[CC(PO),C_{prv}],M_{prv}],[[CC([mr,$k_M\times k_{M_1}$]),M_{prv}],[[CC([r,k_{M_1}]),M_{prv}],[$k_{C_2}^{-1}$,M_{pub}],B,[[PT,$k_{C_1}\times k_{C_2}$],B_{prv}];

(2)TP→C:k_M^{-1} or TP→C:$k_{M_1}^{-1}$;

(2′)TP→M:$k_{C_2}^{-1}$ or TP→C:$k_{M_1}^{-1}$,r^{-1}。

在基本协议中,C 从 TP 下载加密产品后,向 M 发送一系列消息。M 收到消息后,检查是否对 PO 满意。若不满意,M 通知 C 取消协议;若满意,M 发送消息给 C。在第四步,当收到取消协议的消息后,C 取消协议;否则,C 比较收到的消息与下载的加密产品。若不符合,令 M 重新发送或通知 M 取消协议;若符合,发送消息给 M,同时启动一个计时器。若在规定时间内不能收到正确消息,则通知 TP 执行扩展协议;若收到,C 对其检查。若消息正确,则协议正常结束;否则,C 通知 TP 执行扩展协议。

当协议参与方作弊或发生通信故障时执行扩展协议。首先由 C 向第三方发送消息。TP 进行判断,若是 C 的过错,TP 不必采取任何措施;若是 M 的过错,则 TP 要求 M 发送正确消息,并启动一个计时器。若 M 在规定时间内未响应,TP 在(2)中直接发送消息给 C;否则 TP 将收到的消息转发给 C。若 M 的过错由 C 引起,即 M 声称未收到正确的付款,则 TP 要求 M 发送正确消息。之后,在(2′)中,TP 分别发送正确消息给 M 和 C。

3.2 建立模型

本节假设顾客、商家及 TP 均为诚实主体,因此只需执行基本协议。首先利用 LCFSM 为协议建模。将第 i 步中处理的消息记为 m_i,对进程 P 的某个状态 s_i,若 $m\in K_i$,则 $P\ni m\in F_i$。反之,若 $P\ni m\in F_i$,则 $m\in K_i$。由于消息数量较多,公式集中不再明确写出上述公式。此外,K_{P_i}、F_{P_i} 分别表示 P 处理第 i 条消息后的知识集和公式集。

建立顾客进程　在 s_0,K_{C_0} 为(C,TP,PO,PT,k_{C_1},$k_{C_1}^{-1}$,k_{C_2},$k_{C_2}^{-1}$,M_{pub},B_{pub}),F_{C_0} 为($C\succ\xrightarrow{M_{prv}}M$,$C\succ M\ni k_M^{-1}$,$C\succ M\ni k_{M_1}^{-1}$)。C 收到 m_1 后转至 s_1,知识集中增加了 m_1,公式集不变。之后发送 m_2 给 M,转至 s_2,知识集中增加了 m_2,CC(PO),PT,k_{C_1},k_{C_2},[PT,$k_{C_1}\times k_{C_2}$],公式集不变。当收到 M 的 abort1 消息后,C 转至 s_3,之后回到 s_0;当收到 m_3 后,C 到达 s_4。收到 M 的签名消息后,应用 R4 得 $C\ni$[CC(PO),C_{prv}],$C\ni$CC([r,k_{M_1}]),CC([mr,$k_M\times k_{M_1}$])。知识集增加了 m_3,[CC(PO),C_{prv}],CC([r,k_{M_1}]) 及 CC([mr,$k_M\times k_{M_1}$]);应用 R1 得 C≻M→[CC(PO),C_{prv}],C≻M→CC([mr,$k_M\times k_{M_1}$]),C≻M→CC[r,k_{M_1}];进而应用 R5 得 C≻M→[r,k_{M_1}],C≻M→[mr,$k_M\times k_{M_1}$],之后转至 s_6。C 将 CC([r,k_{M_1}])、CC([mr,$k_M\times k_{M_1}$])与下载的加密产品做比较。若不符合,发送 abort2 通知 M 取消协议,转至 s_5;若符合,C 发送 m_4 给 M,转至 s_7,知识集增加了 m_4,公式集不变。收到 m_5 后转至 s_8。之后应用 R3 得 $C\ni k_M^{-1}$,$C\ni r^{-1}$,进而有 $C\ni mr$,$C\ni m$。由 R2 得 C≻M→mr,C≻M→r^{-1},进而有 C≻M→m。在 s_9,C 的知识集增加了 m_5,k_M^{-1},r^{-1},mr,r,m,之后转至 s_0,等待另一轮协议的执行。具体模型如图 1 所示。

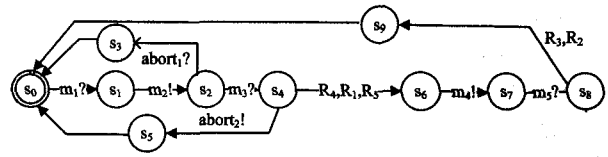

图 1　顾客进程 C

C 的知识集和公式集为

$K_{C_0}=$(C,TP,k_{C_1},$k_{C_1}^{-1}$,k_{C_2},$k_{C_2}^{-1}$,M_{pub},B_{pub});

$F_{C_0}=(C\succ\xrightarrow{M_{prv}}M,C\succ M\ni k_M^{-1},C\succ M\ni k_{M_1}^{-1})$;

$K_{C_1}=K_{C_0}\cup\{m_1\}$;

$F_{C_1}=F_{C_0}$;

$K_{C_2}=K_{C_1}\cup\{m_2$,PO,CC(PO),PT,k_{C_1},;

$F_{C_2}=F_{C_0}$;

$K_{C_3}=K_{C_2}\cup\{m_3$,[CC(PO),C_{prv}],CC([r,k_{C_2},[PT,$k_{C_1}\times k_{C_2}$]}k_{M_1}]),CC([mr,$k_M\times k_{M_1}$])};

$F_{C_3}=F_{C_0}\cup\{C\succ M\to[r,k_{M_1}],C\succ M\to[mr,k_M\times k_{M_1}],C\ni$[CC(PO),$C_{prv}$],$C\succ M\to[mr,k_M\times k_{M_1}],C\ni$[CC(PO),$C_{prv}$],$C\ni$CC([$r$,$k_{M_1}$]),$C\ni$CC([$mr$,$k_M\times k_{M_1}$])};

$K_{C_3'}=K_{C_2}$;$F_{C_3'}=F_{C_2}$;

$K_{C_4}=K_{C_3}\cup\{m_4\}$;$F_{C_4}=F_{C_3}$;

$K_{C_4'}=K_{C_3}$;$F_{C_4'}=F_{C_3}$;

$K_{C_5}=K_{C_4}\cup\{m_4,k_m^{-1},r^{-1},mr,r,m\}$;

$F_{C_5}=F_{C_4}\cup\{C\ni k_M^{-1},C\ni r^{-1},C\succ M\to m\}$。

建立商家进程 M　在 s_0,K_{M_0} 为(M,TP,k_M,k_M^{-1},k_{M_1},$k_{M_1}^{-1}$,C_{pub},B_{pub});F_{C_0} 为($M\succ\xrightarrow{C_{prv}}C$,$M\succ\xrightarrow{B_{prv}}B$,$M\succ C\ni k_{C_1}^{-1}$,$M\succ C\ni k_{C_2}^{-1}$)。若 M 收到 m_2 则转至 s_1,利用 R1 得 M≻C→CC(PO),M≻B→[PT,$k_{C_1}\times k_{C_2}$]。对前者利用 R5 得 M≻C→PO,应用 R6 得 M∋ID(C);对后者,由于 B≻C→[PT,$k_{C_1}\times k_{C_2}$],利用 R7 得 M≻C→[PT,$k_{C_1}\times k_{C_2}$]。利用 R4 得 M∋[PT,$k_{C_1}\times k_{C_2}$],M∋CC(PO),转至 s_2。此时知识集增加了 m_2,PO,CC(PO),[PT,$k_{C_1}\times k_{C_2}$],B,ID(C)。在 s_2,M 检查是否对 PO 满意,若不满意,发送 abort1 通知 C 取消协议,并转至 s_3,之后回到 s_0;若满意,发送 m_3 给 C,并转至 s_4。此时知识集增加了 m_3,[CC(PO),C_{prv}],k_M^{-1},r^{-1},mr,r,m,CC([r,k_{m_1}]),CC([mr,$k_M\times k_{M_1}$]),公式集不变。当收到 abort2 后,转至 s_5,之后回到 s_0;否则,若收到 m_4,转至 s_6,应用 R3 得 $M\ni k_{C_2}^{-1}$ 及 M∋PT。对 M≻C→[PT,$k_{C_1}\times k_{C_2}$],应用 R2 得 M≻C→PT。由 R1 得 M≻C→CC([m,$k_M\times k_{M_1}$])。进一步利用 R5 得 M≻C→[m,$k_M\times k_{M_1}$],转至 s_7。此时知识集增加了 m_4,$k_{C_2}^{-1}$,PT,CC([m,$k_M\times k_{M_1}$])。在 s_7,M 向 C 发送 m_5 后转至 s_8。此时知识集增加了 m_5,公式集不变。之后回到 s_0,等待下一轮协议的执行。建模过程如图 2 所示。

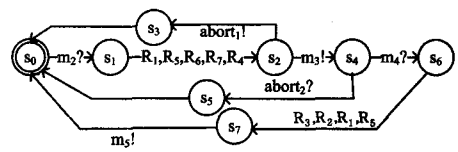

图 2　商家进程 M

下面给出 M 的知识集和公式集。

$K_{M_0}=(M,TP,k_M,k_M^{-1},k_{M_1},k_{M_1}^{-1},C_{pub},B_{pub})$;

$F_{M_0}=(M>\xrightarrow{C_{prv}}C,M>\xrightarrow{B_{prv}}B,M>C\ni k_{C_1}^{-1},M>C\ni k_{C_2}^{-1})$;

$K_{M_1}=K_{M_0}$;$F_{M_1}=F_{M_0}$;

$K_{M_2}=K_{M_1}\cup\{m_2,PO,CC(PO),[PT,k_{C_1}\times k_{C_2}],B,ID(C)\}$;

$F_{M_2}=F_{M_0}\cup\{M>C\to PO,M>C\to[PT,k_{C_1}\times k_{C_2}],M\ni CC(PO),M\ni[PT,k_{C_1}\times k_{C_2}]\}$;

$K_{M_3}=K_{M_2}\cup\{m_3,[CC(PO),C_{prv}],k_M^{-1},r^{-1},mr,r,m,CC([r,k_{M_1}]),CC([mr,k_M\times k_{M_1}])\}$;

$F_{M_3}=F_{M_2}$;

$K_{M_3'}=K_{M_2}$;$F_{M_3'}=F_{M_2}$;

$K_{M_4}=K_{M_3}\cup\{m_4,k_{C_2}^{-1},PT,CC([m,k_M\times k_{M_1}])\}$;

$F_{M_4}=F_{M_3}\cup\{M\ni k_{C_2}^{-1},M\ni PT,M>C\to PT,M>C\to[m,k_M\times k_{M_1}]\}$;

$K_{M_4'}=K_{M_3}$;$F_{M_4'}=F_{M_3}$;

$K_{M_5}=K_{M_4}\cup\{m_5\}$;$F_{M_5}=F_{M_4}$。

建立第三方进程 TP　在 s_0，B 的 K_{TP_0} 为 $(TP,M,k_M,k_M^{-1},C_{pub},B_{pub})$，$F_{TP_0}$ 为 $(TP>\xrightarrow{C_{prv}}C,TP>\xrightarrow{M_{prv}}M)$。TP 将加密产品发给 C，转至 s_1，之后返回 s_0。建模过程如图 3 所示。

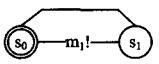

图 3　第三方进程 TP

TP 的知识集和公式集为

$K_{TP_0}=\{TP,M,k_M,k_M^{-1},C_{pub},B_{pub}\}$;

$F_{TP_0}=\{TP>\xrightarrow{C_{prv}}C,TP>\xrightarrow{M_{prv}}M\}$;

$K_{TP_1}=K_{TP_0}\cup\{m_1\}$;$F_{TP_1}=F_{TP_0}$。

3.3　性质的分析

定理 1　AFRFE 协议满足有效性。

证明：当协议成功结束时，由 C 的知识集终态 K_{C_5} 可知 $m\in K_{C_5}$，因此 C 拥有想要购买的商品。同理，由 M 的知识集终态 K_{M_5} 可知 $PT\in K_{M_5}$，所以 M 拥有支付代币。因此，当协议成功结束时，交易可顺利完成，且 C 获得想要的商品，M 获得正确的支付货币。该协议满足有效性。

定理 2　AFRFE 协议满足可追究性。

证明：由 C 的公式集终态 F_{C_5} 可知 $C>M\to m\in F_{C_5}$，即 C 可证明 M 对购买的产品负责。同理，由 M 的公式集终态 F_{M_5} 可知 $M>C\to PT\in F_{M_5}$ 及 $M>C\to PO\in F_{M_5}$，即 M 可证明 C 对支付代币及购买订单负责。因此协议满足可追究性。

定理 3　AFRFE 协议满足公平交换性。

证明：由定理 1 可知，当协议成功结束时，$m\in K_{C_5}$ 且 $PT\in K_{M_5}$，即交换者得到各自所需的东西。

由于协议语句(3)、(4)是可中断的，分析如下：

当(3)中断时，C 的知识集为 $K_{C_3'}=K_{C_2}=K_{C_1}\cup\{m_2,PO,CC(PO),PT,k_{C_1},k_{C_2},[PT,k_{C_1}\times k_{C_2}]\}$，因此 $m\notin K_{C_3'}$。M 的知识集为 $K_{M_3'}=K_{M_2}=K_{M_1}\cup\{m_2,PO,CC(PO),[PT,k_{C_1}\times k_{C_2}],B\}$，因此 $PT\notin K_{M_3'}$。当(4)中断时，由 C 的知识集 $K_{C_4'}$ 可知 $m\notin K_{C_4'}$。由 M 的知识集 $K_{M_4'}$ 可知 $PT\notin K_{M_4'}$。

综上所述，协议满足公平性。

定理 4　AFRFE 协议满足确认接收性。

证明：检查付款前 C 的公式集 F_{C_3} 可知 $C>M\to[r,k_{M_1}]\in F_{C_3}$ 及 $C>M\to[mr,k_M\times k_{M_1}]\in F_{C_3}$。从而在付款前 C 可证明 M 对发送的加密产品负责。此外，由协议描述，只有 C 确认加密产品与其从 TP 处下载的加密产品相符合时才会发送支付代币的解密密钥给 M。因此协议满足确认接收性。

定理 5　AFRFE 协议不满足顾客匿名性。

证明：由 M 的知识集终态 K_{M_5} 可知 $ID(C)\in K_{M_5}$，所以当协议成功结束时，M 拥有 C 的身份。因此协议不满足顾客匿名性。

4　分析协议的其他性质

上节使用扩展模型分析了 AFRFE 协议的常见安全性质，但无法分析活性及时效性，且假设顾客和商家均为诚实主体。由于活性及时效性与参与者拥有的知识及公式无关，因此本节取消对顾客和商家的假设。对上节模型抽象后进行简单修改，用时间自动机为协议建模，并用 UPPAAL 验证协议的公平性、时效性与活性。这里假定顾客等待解密密钥的时间界限为 5s。

4.1　为参与者建模

建立顾客进程 C　C 在初始状态 s_0 从 TP 下载到 m_1 后，转至 s_1，之后发送 m_2 给 M，并转至 s_2。当从 M 收到取消协议的通知 abort1 后，C 转至 s_3；否则收到 m_3 后，将其与下载的加密产品比较。若不符合，则令 M 重新发送 m_2 或发送 abort2 通知商家取消协议；若符合转至 s_8，并发送 m_4 给 M。同时 C 设置一个计时器，转至 s_9。若在规定的 5s 内未收到 m_5，转至 s_{10}，之后通知 TP 执行扩展协议。当收到 m_{6_1} 或 m_8 时，C 重置计时器和 compare 的值，并回到 s_0。否则，若 C 在规定的 5s 内收到 m_5，马上对其检查，到达 s_{15}。若是正确的解密密钥，转至 s_{17}；否则，C 通知 TP 执行扩展协议。建模过程如图 4 所示。

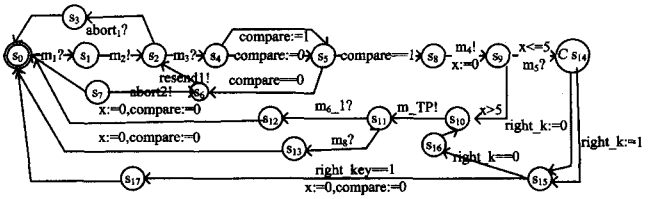

图 4 顾客进程

建立商家进程 M　M 在初始状态 s_0 收到 m_2 后转至 s_1，并检查是否对 PO 满意，转至 s_2。若不满意，M 转至 s_3，之后通知 C 取消协议；否则，M 发送 m_3 给 C，转至 s_6。在 s_6，若收到重新发送 m_3 的通知，回到 s_5；若收到 m_4，则对加密的 PT 解密，并检查随机数的新鲜性。若随机数不新鲜，转至 s_{10}，并等待 resend 消息的到来。当收到该消息后，M 发送 m_{6_0} 给 C；当收到 m_7 后，转至 s_{13}，并最终返回 s_0；否则，若随机数新鲜，转至 s_{14}。在 s_{14}，C 可以等待 resend3 的到来，也可以发送 m_5。对于前者，M 发送 m_{6_0}，并最终回到 s_0；对于后者，发送 m_5 之后，M 转至 s_{17}。此时，若发送的是正确的解密密钥，则正常终止协议并回到 s_0；否则 TP 执行扩展协议。建模过程如图 5 所示。

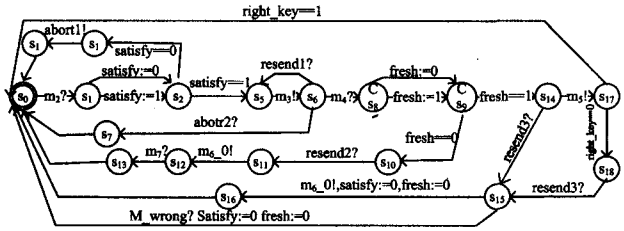

图 5　商家进程

建立第三方进程 TP　在初始状态 s_0，TP 向 C 发送 m_1 并转至 s_1，之后返回 s_0。在 s_0，若收到 $m_{\_TP}$，转至 s_2。若 C 发送的 PT 不新鲜，TP 通知 M 重新发送 $k_{M_1}^{-1}$，收到后 TP 在 s_7 发送 $k_{C_2}^{-1}$ 给 M，并发送 $k_{M_1}^{-1}$ 给 C，转至 s_9，并最终返回 s_0。若随机数不新鲜，TP 要求 M 重新发送 $k_{M_1}^{-1}$，并启动计时器，转至 s_4。若在 5s 内收到 $k_{M_1}^{-1}$，转至 s_5；否则发送 k_M^{-1} 给 C，转至 s_{10}，并通知 M 顾客有欺骗行为，返回 s_0。建模过程如图 6 所示。

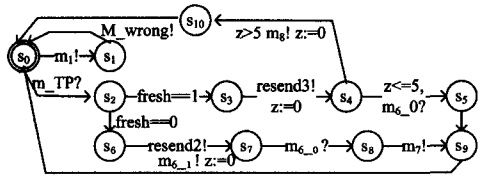

图 6　第三方进程

整个系统为三者之积 C || M || TP。大致工作过程为：TP 发送 m_1 给 C，C 收到后发送 m_2 给 M，之后 M 发送 m_3 或 abort1 给 C，C 收到 abort1 后取消协议，否则发送 m_4 给 M，M 收到 abort2 后取消协议，否则发送 m_5 给 C。

4.2　性质分析

在模拟器中观察各进程之间的交互情况，初步判定模型符合协议要求。在验证器中的验证结果如图 7 所示。

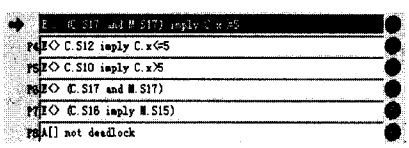

图 7　UPPAAL 验证器中的结果

(1)A[] not deadlock 通过验证，表明系统没有死锁。

(2)E<>(C. s_{17} and M. s_{17}) 通过验证，表明 C 收到了期望的商品，M 收到了正确的支付代币。

(3)E<>(C. s_{16} imply M. s_{15}) 通过验证，表明若 C 收到的解密密钥不正确，则 M 必须重发产品的解密密钥。

(4)E<>(C. s_{10} imply C. $x>5$) 通过验证，表明若 C 在规定时间不能收到产品的解密密钥，则通过 TP 解决问题。

(5)E<>(C. s_{10} imply C. $x<=5$) 通过验证，表明若 C 收到了产品的正确的解密密钥，则时间必定不超过 5s。

(6)E<>(C. s_{17} and M. s_{17}) imply C. $x<=5$ 通过验证，表明 C 在规定时间收到了期望的商品，M 收到了正确的支付代币。

定理 6　AFRFE 协议满足活性。

证明：由验证结果(1)可知协议满足活性。

定理 7　AFRFE 协议满足有效性。

证明：由验证结果(2)可知协议满足有效性。进一步验证了 3.3 节的证明结果。

定理 8　AFRFE 协议满足公平性。

证明：由验证结果(2)、(3)、(6)可知协议在顾客和商家不是诚实主体的情况下依然满足公平性，进一步验证了 3.3 节的证明结果。

定理 9　AFRFE 协议满足时效性。

证明：由验证结果(4)、(5)可知协议满足时效性。

结束语　本文提出了带有逻辑推理能力的通信有限状态自动机，扩展自动机的状态带有知识集分量和公式集分量，其中知识集用于表示协议参与者自身拥有的知识，公式集用于模拟逻辑推理能力，从而可分析带有加密、签名等复杂消息的协议的基本安全性质。对模型抽象并修改后，验证了协议的活性和时效性。下一步工作是利用扩展模型修改 UPPAAL，使其适用于自动验证电子商务协议特有的安全性质。

参 考 文 献

[1] Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR[C]// Itshape Proceedings of TACAS. LNCS 1055. Springer-Verlag, 1996: 147-166

[2] Heintze N, Tygar J, Wing J, et al. Model Checking Electronic Commerce Protocols[C] // Proceedings of the 2nd USENIX Workshop in Electronic Commerce. November 1996: 146-164

[3] Ouyang C, Billington J. An improved formal specification of the Internet Open Trading Protocol[C]// Proceedings of the 2004 ACM Symposium on Applied Computing. Nicosia, Cyprus, 2004: 779-783

[4] Díaz G, Cuartero F, Ruiz V V, et al. Automatic verification of the TLS handshake protocol[C]// SAC. 2004: 789-794

[5] Kailar R. Accountability in electronic commerce protocols[J]. IEEE Transaction on Software Engineering, 1996, 22(5): 313-328

[6] 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

[7] 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

[8] Kremer S. Formal Analysis of Optimistic Fair Exchange Protocols[D]. Universit'e Libre de Bruxelles Facult'e des Sciences, 2003-2004

[9] 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

[10] 王茜，杨德礼. 验证电子商务协议的新逻辑分析方法[J]. 系统工程学报，2009，24(1)：32-38

[11] 刘义春，张焕国. 电子商务协议的串空间分析[J]. 计算机科学，2008，2(1)：09-114

[12] Ray I, Ray I, Natarajan N. An anonymous and failure resilient fair-exchange ecommerce protocol[J]. Decision Support Systems, 2005, 39: 267-292

[13] Brand D, Zafiropulo P. On Communicating Finite State Macines [J]. Journal of the Association for Computing Machinery, 1983, 30(2): 323-342

[14] Larsen K G, Petterson P, Wang Yi. UPPAAL in a nutshell[J]. Journal on Software Tools for Technology Transfer, 1997, 1(1/2): 134-152