软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):509−521 [doi: 10.3724/SP.J.1001.2011.03945]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

公平交换协议形式逻辑*

陈 明[1+], 吴开贵[1], 吴长泽[1], 徐 洁[1,2], 吴中福[1]

[1](重庆大学 计算机学院,重庆 400044)

[2](School of Computing, University of Leeds, UK)

Formal Logic for Fair Exchange Protocols

CHEN Ming[1+], WU Kai-Gui[1], WU Chang-Ze[1], XU Jie[1,2], WU Zhong-Fu[1]

[1](College of Computer Science, Chongqing University, Chongqing 400044, China)

[2](School of Computing, University of Leeds, UK)

+ Corresponding author: E-mail: chenming9824@yahoo.com.cn

Chen M, Wu KG, Wu CZ, Xu J, Wu ZF. Formal logic for fair exchange protocols. *Journal of Software*, 2011, 22(3):509−521. http://www.jos.org.cn/1000-9825/3945.htm

Abstract: The fairness and punctuality of optimistic fair exchange protocols are difficult to analyze by using belief logic. Based on the studies of existing formal models and security attributes in fair exchange, a formal model for logic reasoning and fair exchange protocols is proposed. In the model, the channel errors are transferred to the attacker's behaviors, the participants are divided into honest and dishonest ones, and the threats are attributed to two types of intruders. Based on the idea of model checking, the protocols are defined as an evolved system that has the Kripke structure, and the parties are considered as processes in an asynchronous environment. The new logic stimulates the time operators to control the transfers among the participants' behaviors and is simple and easy to use. Through typical optimistic fair exchange protocols, the article demonstrates the course of protocol analysis. Two flaws of the protocol are discovered and improved. The case study shows that the new logic can be used to analyze the fairness and timeliness of fair exchange protocols.

Key words: asynchronous communication; fair exchange; formalize analysis; logical reasoning; model checking

摘 要: 在深入分析公平交换协议现有研究和各项安全属性的基础上,由于信任逻辑方法难以分析乐观公平交换协议的公平性和时限性,提出一种公平交换协议形式化模型和推理逻辑.新模型将信道错误转化为攻击行为,将参与者分为诚实与不诚实两类,并将这些威胁归结为两类入侵者.基于模型检查思想,新逻辑将协议定义为Kripke结构的演化系统,将参与者看作异步环境中的通信进程,定义了时间算子控制实体行为的转换.同时,新逻辑继承了信任逻辑简单、实用的优点.以一个典型协议为例,采用逻辑结合模型检查的方法,演示了分析协议的过程.发现并改进了协议实例的安全缺陷.案例分析表明,新逻辑能够分析公平交换协议的公平性和时限性.

关键词: 异步通信;公平交换;形式化分析;推理逻辑;模型检查

中图法分类号: TP309 **文献标识码**: A

* 基金项目: 国家自然科学基金(90818028); 国家科技支撑计划(2008BAH37B04)
收稿时间: 2009-11-05; 定稿时间: 2010-09-06

随着电子商务应用的不断发展,公平交换问题日益受到人们的广泛关注.公平交换问题是关于参与者对有价值数据公平交换的问题.公平交换协议的目的就是解决公平交换问题,目标是实现数据交换而又不会使一方比另一方有获取更多信息的优势,促使互不信任的合作伙伴公平完成交换.在实际应用中,公平交换协议涉及电子商务、数字合同签名、不可否认协议和签收电子邮件等.

由于对可信第三方(TTP)的依赖较轻,乐观公平交换协议成为了公平交换协议研究的主要方向.乐观公平交换的概念由 Asokan 等人提出,采用离线的可信第三方(off-line TTP)确保交换的公平性,他们对该类型协议进行了大量研究[1,2].另外,Bao 等人[3]提出采用 CEMBS 在无需恢复签名消息的情况下验证签名的正确性.Ray 等人[4]提出了采用交叉验证理论进行被交换电子项的验证,以实现自动争端解决.Pagnia 等人[5]将交换实体看作异步环境下的通信进程,采用多模块组合方式实现不同公平性等级交换协议.Wang 等人[6]提出在异步通信条件下基于离线 TTP 的容错交换协议,采用 GDH 签名方案和消息日志方法,使得协议具有信道和本地系统错误的恢复能力.Hernandez-Ardieta 等人[7]采用签名策略的方法解决异步环境下的乐观公平交换问题,签名策略是一组创建签名和验证签名的规则,使得商品购买者可在交换前判断卖家是否可信.另外,Kremer[8],Zhou[9]等人对不可否认协议进行了大量的研究.

形式化验证技术是公平交换协议分析和设计的重要手段.Kailar[10]在 BAN 逻辑[11]基础上提出了 Kailar 逻辑方法,使得协议主体能够向第三方证明另一方对某个公式负责;Zhou 等人[12]采用 SVO 逻辑[13]方法分析协议的不可否认性;Schneider[14]使用 CSP 方法、Bella 和 Paulson[15]应用 Paulson 的归纳法,分别对 ZG(96)不可否认性协议[16]进行了分析.上述逻辑方法用于证明协议的不可否认性,但难以分析协议的公平性和时限性.Shmatikov 等人[17]使用基于模型检查的有限状态机(Murφ)对 ASW 合同签名协议[2]和 GJM 协议[18]行了分析,发现了其中存在的安全缺陷.Kremer 等人[19]采用基于博弈理论的 ATL 方法分析公平交换协议,采用自动验证技术分析了 ASW 协议[2]、ZG(97)协议[9]和 KM 协议[8].Dashti[20]应用进程代数来形式化描述交换协议,采用基于模态逻辑的有限状态模型检测器来验证协议的行为是否符合其目标.卿斯汉和李改成[21]提出了一个公平交换协议的形式化模型,使用标准的 Z 语言规范作为协议描述工具,并用以分析了 Asokan 提出的 APR 协议[1],发现了该协议存在的漏洞.模型检查方法可以分析协议的公平性,但建模方法和状态空间爆炸是其最大难点.

方法虽然很多,但是到目前为止,还没有一种方法能够全面描述公平交换协议的所有性质,新的研究着眼于综合多种方法以发现更多的攻击.本文工作主要针对具有复杂结构的乐观型电子商务协议,基于模型检查思想和知识推理逻辑构建了公平交换协议的新形式化逻辑方法.新方法重点解决协议分析中的信道问题和时间敏感性问题.

信道问题是公平交换协议分析中一个重要问题.在开放的网络环境下,实体间的消息交互可看作异步环境下进程间的通信,进程在不完全可靠的信道上发送和接收消息,对消息进行缓存和处理.消息在信道上传输的过程中受到各种威胁,包括信道错误和恶意实体的主动攻击.信道错误导致消息的丢失、错误或被延迟,恶意实体能窃听、拦截、篡改和延迟消息.另外,不诚实的交换实体可以主动终止或推迟消息的发送,发送错误的消息.为简化问题,一种被广为接受的方案是,将上述问题归结为消息传输过程中的信道问题,将信道划分为 3 类[1]:可靠信道、可恢复信道和不可靠信道.可靠信道要求消息在确定的时间范围内正确到达指定的接收者,可恢复信道假设消息在有限但不可预知的时间范围内正确到达指定的接收者,而不可靠信道则不保证消息能够正确到达指定的接收者.异步通信环境对应于可恢复信道和不可靠信道,假设交换双方之间的信道为不可靠信道,而交换实体与 TTP 之间的信道为可恢复信道.这种信道假设虽然简化了协议分析的复杂度,但是不利于协议的形式化描述.本文通过定义新的形式化模型,将信道问题映射为不同的 Dolev-Yao[22](以下简写为 DY)攻击者模型,信道错误等价于信道受到 DY 攻击者的控制.

时间敏感性是公平交换协议分析的另一主要问题.消息到达指定接收者的顺序和时间点,以及消息的有效期等时间属性都对协议的正确性具有重要影响.例如,韩志耕[23]报道了 ZG(96)协议[16]的时限性缺陷.通过在新的形式化逻辑中引入时间算子和消息有效性验证公式,满足协议时限性分析的需要.

本文将公平交换协议定义为具有 Kripke 结构的演化系统,定义了融合 BAN-Like 逻辑[11,13]思想的知识推理

逻辑.给定初始状态、命题集合以及状态到命题的映射,基于模型检测的思想,采用新逻辑方法检查协议实例可能存在的演化路径.如果所有路径都能保持协议的公平性,协议被认为是安全的.作为案例,本文分析了一个典型的乐观型电子商务协议[5],首次发现了协议实例中的安全缺陷,讨论了形成攻击的原因并提出改进意见.结果表明,新的逻辑方法可用于分析公平交换协议的公平性和时限性.

1 公平交换协议安全属性分析

公平交换协议应具有的安全属性没有标准定义,本文引用一种被广为接受的非形式化定义方案[2,5].

假设有两个协议参与者 A(Alice)和 B(Bob),他们分别拥有待交换的电子项 i_X 及其描述 d_X,这里,$X=A$ 或 $X=B$.假设存在可验证函数 $f(*)$,使得 $d_X=f(i_X)$.协议有成功和终止两种结束状态,参与双方可判定自身的结束状态.

在异步网络环境下,对于诚实实体 A(不可判定 B 是否诚实),只有在确认已收到期望的电子项 i_B 后才愿付出自己的电子消息 i_A;反之,对于诚实实体 B 也是同样情形.这就形成了一个不可调和的矛盾:A,B 谁都不愿先付出自己的电子项,那么最终谁也得不到期望的电子项.针对这个矛盾问题,一种有效的解决方案是,双方都将自己的消息交给一个可信第三方实体(TTP),要么通过 TTP 中转,要么在出现争议的时候让 TTP 进行裁决和补偿.中转方式,即 In-line TTP 或 On-line TTP 模式,需要 TTP 大量参与,于是,TTP 的性能和安全性受到广泛地质疑;补偿方式,即 Off-line TTP 模式,必然有一方要在还没有获得期望的信息之前就需要先付出自己的信息,当他在随后没有收到期望的电子项时,就可以向 TTP 申请补偿.这时候,向 TTP 提交证据以证明自己的行为就显得特别重要.因此,公平交换协议的主要安全属性有:有效性(effectiveness)、公平性(fairness)和时限性(timeliness).

定义 1(有效性). 设两个参与实体都是诚实的,双方都不放弃交换,且可验证 i_X 满足其描述 d_X,那么当协议结束时,A 获得 i_B,B 获得 i_A,且双方都到达成功状态.

定义 2(公平性). 假设 A 是诚实的,当协议结束时,除非 A 获得 i_B 且 $d_B=f(i_B)$,否则 B 不能获得关于 i_A 的任何有用信息;反之亦然.

定义 3(时限性). 假设 A 是诚实的,那么在协议开始时,A 能够确定交换协议将在某个有限的时间段内结束,而在协议结束时,A 要么到达成功状态,要么到达终止状态,且不影响公平性;反之亦然.

有效性定义中,要求“双方都不放弃交换”的前置条件对于异步通信环境来说是脆弱的[5].因为在异步网络环境下,消息在信道上的延迟时间是不可预知的(任意但有限).当诚实参与者 A 在某一时刻没有收到期望的消息 m 时,A 不能判定:m 是由于信道原因被延迟了,或者是 B 根本没有发送 m.此时,A 只能等待 m,只要 A 还在等待,那么成功或终止状态都是可能的.在实际的应用中,A 不可能永远等待消息 m.另外,Pagnia 等人认为,交换协议要满足公平性还应具有电子项 i_X 可产生性(generatability)和可撤销性(revocability)[5].可产生性是指能够确保 TTP 可产生电子项 i_X;而可撤销性是指 TTP 可撤销电子项 i_X,如撤销支付.

前面定义中不包含传统的安全属性,如机密性和认证性等,这是由于交换协议通常是建立在认证协议(如 TLS 协议)基础上的应用层协议,甚至有些交换协议会隐匿参与者的确切身份,如匿名交换协议就要求协议具有匿名性[4].可是,从有效性和公平性定义中可以发现,在分析协议的这些属性时是隐含了对电子项 i_X 的认证需求的,如:有效性假设“可验证项 i_X 满足其描述 d_X”,公平性要求验证“$d_X=f(i_X)$”.基于此,本文提出电子项 i_X 的认证属性,即电子项 i_X 符合其描述 d_X 的属性,称为一致性(uniformity).

定义 4. 具有如下性质的函数 $f(*)$是一个安全的单向映射函数:

- 如果 $m,m'\in\Omega$,那么 $f(m)=f(m')\Rightarrow m=m'$.这里,$\Omega$表示二进制形式的消息集合,且$f(m),f(m')\in\Omega$;
- 不存在多项式时间函数 $F(*)$使得 $F(f(m))=m$.

定理 1. 假设 T 是受诚实实体 X 信任的可信第三方,k_T 是 T 用于签名的密钥,且 $k_T\notin K_I$(K_I 表示攻击者的密钥集),d_B 是 i_B 的描述,如果 X 可验证 d_B 是由 k_T 签名的,那么 X 相信 d_B 是 i_B 的合法描述.

证明:定理 1 的正确性是显然的.实体 X 不能直接判断 d_B 的真伪,只能通过一个可信第三方的保证来判定 d_B 是否可信.根据签名属性,如果 k_T 是 T 的安全签名密钥($k_T\notin K_I$),T 不与任何交换实体 Y 合谋[24],那么 T 对 d_B 的签名表明 d_B 是 i_B 的合法描述(这里,假定可信第三方预先对电子项及其描述进行审查). □

定义 5(一致性). 假设 $f(*)$是安全单向映射函数,d_X是 i_X的合法描述,如果可验证 $d_X=f(i_X)$,则协议具有一致性.

一致性定义明确两点:第一,需要一个安全的单向映射函数 $f(*)$,如单向散列函数,并利用 $f(*)$对 i_X进行一致性验证;第二,d_X是 i_X的合法描述,即 d_X受到可信第三方或权威机构的签名确认.只有同时满足这两方面的要求,才认为协议具有一致性.一致性是其他各项属性的基础,如果协议不满足一致性,那么协议公平性将受到威胁.

2 公平交换协议新形式化逻辑

BAN 类逻辑[11,13]是一种影响广泛的安全协议形式化逻辑,本文融合了 BAN 类逻辑的思想,提出基于知识推理并随时间演化的逻辑系统.

2.1 新的形式化模型

为了准确地定义形式化模型,表 1 归纳了公平交换协议存在的 3 类攻击实体的攻击行为(信道错误同样会对公平交换协议造成危害[1],因此将信道错误看作一种被动攻击行为).

Table 1 Analysis of the attacker's behaviors

表 1 攻击实体的行为分析

	DY intruders	Dishonest participants	Channel errors
Behaviors	Delay Modify or forge Intercept Replay	Delay Forge Do not send Replay	Delay (resilient and reliable) Bit errors (reliable) Lose (reliable) /

表 1 中,每一行的 3 种攻击行为造成相同的攻击结果.根据信道假设[1],将这 3 种攻击实体归结为标准 DY 攻击者(控制无 TTP 参与的所有子协议)和弱 DY 攻击者(控制有 TTP 参与的所有子协议,本文主要研究对象为有 TTP 参与的公平交换协议,因为这类型协议更复杂,且无 TTP 参与的交换协议已被证明不满足公平性[25])两类.标准 DY 攻击者模型请见文献[22].

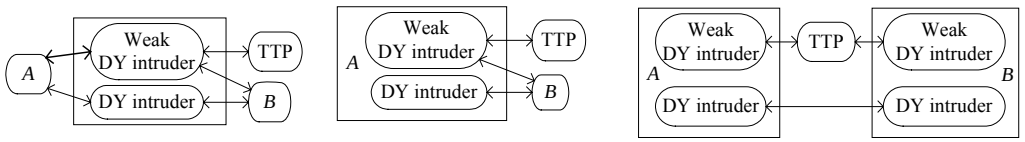
定义 6(弱 DY 攻击者). 一个弱 DY 攻击者能延迟、篡改/伪造和重放信道上传输的消息,但是他不能阻止任何消息到达指定的接收者.

公平交换协议的攻击者模型可分为图 1 所示的 3 类.协议参与者被分为诚实实体(假设 TTP 总是诚实的)和不诚实实体两类,不诚实的实体被看成(弱)DY 攻击者,他控制着通信信道,期望以不诚实甚至是恶意的行为来获得交换中的优势.模型(a)中,参与者 A 和 B 都诚实,攻击者仅是一个外部攻击者.模型(b)中,不诚实实体 A 被看成一个内部攻击者,他的攻击目标是诚实实体 B.模型(c)中,A 和 B 都是不诚实的,他们彼此攻击.模型(a)/模型(c)中,两个实体的能力对等,尤其模型(a)中并未考虑不诚实实体的行为.模型(b)中,B 总是和攻击者进行通信,TTP 和 A 都不可见,而 A 作为 DY 攻击者,直接与 B 和 TTP 进行信息交互,且作为弱 DY 攻击者控制着 B 和 TTP 之间的通信.显然,3 类模型中,模型(b)的攻击能力是最强的,形成能力不对等的局面,诚实实体面临最大的安全威胁.据此,我们做出如下合理假设.

假设 1. 如果公平交换协议 Σ在攻击模型(b)下是可证明安全的,那么 Σ在模型(a)/模型(c)下也是可证明安全的.

根据假设 1,本文采用攻击模型(b),分别从诚实实体和不诚实实体两方面来分析协议的安全性.诚实实体的目标是确保公平性,他在付出电子项的同时,期望能确保收到正确的电子项;而不诚实实体的目标是打破公平性,在已获得电子项的同时不付出自己的电子项.

本文模型的核心思想是:每个诚实实体根据发送、接收和已有的消息判定自身状态,对其他实体的行为和状态不可判定.其他实体对当前实体是不可见的,因此,本文引入(弱)DY 攻击者来模拟这一现象.当出现表 1 中所示攻击行为结果时,本文不考虑具体行为实体,将其全部归结为攻击者的行为.这样,将信道问题和参与者的行为属性都转化为攻击者模型,并与经典攻击模型合而为一.



(a) Both participants are honest (b) One of participants is dishonest (c) Both participants are dishonest
(a) 两个参与者都是诚实的 (b) 存在一个不诚实的参与者 (c) 两个参与者都是不诚实的

Fig.1 Attacker models of fair exchange protocols

图 1 公平交换协议攻击者模型

2.2 知识推理逻辑

2.2.1 逻辑定义

定义 7. 一个公平交换系统(FES)是一个五元组$\Sigma=\langle \Pi,\Psi,\Im,\sigma,\rho\rangle$:

- Π表示所有参与者标识的集合;
- Ψ表示所有命题的集合,Ψ_{AP}表示原子命题集合;
- $\Im$表示非空的有限状态集合,$\Im_0$表示初始状态集合;
- $\sigma:\Im\to 2^{\Psi}$表示状态到命题集合的映射,即将每个 $s\in\Im$映射到一组值为真的命题;
- $\rho\subseteq\Im\times\Im$表示状态迁移函数,对于$\forall s\in\Im,\exists t\in\Im$使得$(s,t)\in\rho$.

公平交换系统由实体、状态和命题组成,状态到命题的映射由具体协议定义,状态迁移是指具有时序关系和因果关系的两个状态之间的转换.公平交换系统的一条运行路径是指满足协议定义的一组有限的状态转换序列,即 $Path_{\Sigma}=s_0,s_1,s_2,\ldots$.这里,$s_0\in\Im_0$表示初始状态,且对于 $i>0$ 的所有 s_i 满足$(s_{i-1},s_i)\in\rho$.

定义 8. 项集$\Omega=\{\{0,1\}^{\omega}\}$由下面 3 类集合组成:$\Pi\subseteq\Omega$,包含所有参与者标识符;$M\subseteq\Omega$,包含所有可预定义的消息文本;$K\subseteq\Omega$,包含所有参与者的密钥.密钥集($K$)又分为下面 4 类无关集合:加密密钥集($K_{enc}$);解密密钥集($K_{dec}$);签名密钥集($K_{sig}$);签名验证密钥集($K_{ver}$).

另外,本文采用 K_X 表示参与者 X 的密钥集($X\in\Pi$).特定地,$k_{x\cdot sig}$ 表示 X 的签名密钥.项集定义了公平交换系统的消息空间,由参与者标识符、密钥和符合协议定义的任何消息文本组成.其中,$\Pi\cap K=\varnothing$,$\Pi\cap M\neq\varnothing$且 $K\cap M\neq\varnothing$.

定义 9. 参与者可自由执行的消息运算定义如下:

- $H(m):\Omega\to\Omega$,表示散列运算;
- $E_k(m):\Omega\times K_{enc}\to\Omega$,表示加密运算;
- $D_k(m):\Omega\times K_{dec}\to\Omega$,表示解密运算;
- $S_k(m):\Omega\times K_{sig}\to\Omega$,表示签名运算;
- $V_k(m):\Omega\times K_{ver}\to\Omega$,表示签名验证运算;
- $\Omega\times\Omega\to\Omega$,表示消息连接运算;
- $\Omega\to\Omega\times\Omega$,表示消息拆分运算.

定义 10. $\Im$表示非空的有限状态集合,$s\in\Im$是一个四元组$\langle A,\varepsilon,\Gamma,t\rangle$:

- $A\in\Pi$,表示参与者的标识符;
- $\varepsilon\in\{Ini,Wai,Act,Abo,Suc\}$,表示状态描述;
- $\Gamma\subseteq\Omega$,表示 A 在当前状态下拥有的知识集;
- $t\in\{0,1,\ldots,n\}$,表示当前状态的时间点,由一组离散的时间序列组成.

状态集$\Im$是所有状态的集合,每个状态元素 s 表示一个本地状态,用一个四元组$\langle A,\varepsilon,\Gamma,t\rangle$描述,表示参与者 A 在时刻 t 的进程状态ε和拥有的知识集Γ.其中,ε是状态描述,$\varepsilon\in\{Ini,Wai,Act,Abo,Suc\}$分别表示进程的初始、等待、活跃、终止(结束)和成功(结束)这 5 种状态.本文将协议参与者定义为具有本地存储和处理能力的通信进程,因此定义这 5 种状态来刻画协议执行过程中参与者的本地状态.其中,*Abo* 和 *Suc* 对应于协议运行的两种结束状态.

系统在 t 时刻的全局状态由 t 时刻的所有本地状态组成.符号 $s_{x\cdot i}$ 表示实体 $x\in\Pi$在 $t=i$ 时刻的状态,$t=0$ 时为初始状态.

定义 11. Ψ_{AP} 是原子命题的集合,定义如下(其中,$m\in\Omega$,$k\in K$,$A\in\Pi$,φ是命题):

- $A\ni m$,表示 A 产生消息 m;
- $A\triangleright m$,表示 A 发送消息 m;
- $A\triangleleft m$,表示 A 接收消息 m;
- $A\propto m$,表示 A 验证消息 m 有效;
- $\oplus Timer$,表示计时器开始计时;
- $\otimes Timer$,表示计时器复位,停止计时;
- $\Diamond Timer$,表示计时器超时;
- $\perp m$,表示 m 在当前时刻有效,相对应的,$\neg\perp m$ 表示 m 在当前时刻无效;
- $k_1\equiv k_2$,表示 k_1 和 k_2 是一对公私密钥对,当 $k_1=k_2$ 时表示其为对称密钥;
- $A\succ\varphi$,表示 A 信任命题φ为真.

原子命题定义了参与者行为、消息项属性和时间操作符.与现有逻辑系统比较,通过引入消息有效性命题($\perp m$)来描述与时间相关消息的属性,这些消息只可能在一定的时间段内有效,如电子商务协议中的支付凭证.参与者有 3 种行为:发送消息、接收消息和产生新消息,分别用$\triangleright$/$\triangleleft$/$\ni$表示.计时器(Timer)描述进程事件,用于触发参与者进程在等待和活跃两个状态之间转换.计时器有 3 种状态:开启、关闭和超时,分别用$\oplus Timer$,$\otimes Timer$ 和 $\Diamond Timer$ 表示.当进程发送消息后,进入等待接收消息状态,计时器开启($\oplus Timer$);当进程正确接收等待的消息时,计时器关闭($\otimes Timer$),进程从等待状态恢复到活跃状态;当参与者进程在规定的最大等待时间内未能正确接收等待的消息时,计时器进入超时状态($\Diamond Timer$).此时,计时器将唤醒参与者进程,进程根据协议定义将终止协议或者请求争端解决.本文采用事件触发状态改变表达式:$Event\Rightarrow s_{x\cdot new}$,表示事件 E 触发实体 x 产生新的状态 $s_{x\cdot new}$.

定义 12. FES 逻辑中命题由如下递归定义:

- 原子命题 $p\in\Psi_{AP}$;
- $\neg\varphi$,$\varphi\wedge\gamma$或$\varphi\vee\gamma$,这里,φ和γ是命题.

下面给出 FES 逻辑命题的正确性条件.给定一个协议运行 R,命题$\varphi\in\Psi$在状态 s 下为真记为:$R|s_t\models\varphi$.下文中,当给定 R 时,简记为 $s_t\models\varphi$.命题真值条件定义如下:

- $s_t\models A\triangleleft m$,当且仅当状态 s_t 下 m 是 A 等待接收的消息;
- $s_t\models A\triangleright m$,当且仅当状态 s_t 下 A 发送了 m;
- $s_t\models A\propto m$,当且仅当状态$\forall s_{t'|t'\geqslant t}$ 下 A 验证 m 有效;
- $s_t\models A\ni m$,当且仅当状态 s_t 下 A 可产生 m;
- $s_t\models\oplus Timer_A$,当且仅当状态 $s_{t'|t'=t-1}$ 下 A 发送了 m,且等待接收消息;
- $s_t\models\otimes Timer_A$,当且仅当状态 $s_{t'|t'=t-1}$ 下 A 正确接收了等待的消息;
- $s_t\models\Diamond Timer_A$,当且仅当在状态 s_t 下,A 在规定的最大等待时间内未能正确接收等待的消息;
- $s_t\models\perp m$,当且仅当在状态 s_t 下 m 有效;
- $s_t\models k_1\equiv k_2$,当且仅当在状态 $s_{t'|t'\geqslant 0}$ 下,k_1 和 k_2 是一对密钥对;
- $s_t\models A\succ\varphi$,当且仅当$\exists s_{t'|0\leqslant t'\leqslant t}\models\varphi$;
- $s_t\models\neg\varphi$,当且仅当 $s_t\models\varphi$;
- $s_t\models\varphi\wedge\gamma$,当且仅当 $s_t\models\varphi$且 $s_t\models\gamma$;
- $s_t\models\varphi\vee\gamma$,当且仅当 $s_t\models\varphi$或 $s_t\models\gamma$.

2.2.2 推理公理

本文的推理逻辑基于模态逻辑,主要采用如下推理规则:$\gamma\wedge(\gamma\rightarrow\varphi)\rightarrow\varphi$.这里$\gamma,\varphi\in\Psi$.

推理规则表达的意思是:已知γ为真,且由γ可推断φ,那么可推断φ为真.基于此推理规则,推理公理定义如下:

- Ax1:$A\triangleleft m\rightarrow m\in\Gamma_A$

Ax1 表示:A 接收消息 m,则 m 纳入 A 的知识集Γ_A.

- Ax2:$A \ni m \rightarrow m \in \Gamma_A$

Ax2 表示:A 产生消息 m,则 m 纳入 A 的知识集Γ_A.A 根据自身已有知识,可采用定义 9 中运算递归产生任意的新消息.

- Ax3:$m||n \in \Gamma_A \rightarrow m \in \Gamma_A \wedge n \in \Gamma_A$

Ax3 表示:如果 m 和 n 的连接消息属于知识集Γ_A,那么 m 和 n 分别属于Γ_A.

- Ax4:$m \in \Gamma_A \wedge n \in \Gamma_A \rightarrow m||n \in \Gamma_A$

Ax4 表示:如果 m 和 n 分别属于知识集Γ_A,那么其连接消息属于Γ_A.

- Ax5:$m \in \Gamma_A \rightarrow H(m) \in \Gamma_A$

Ax5 表示:如果 m 属于知识集Γ_A,那么其散列值也属于Γ_A.

- Ax6:$m \in \Gamma_A \wedge k_{enc} \in \Gamma_A \rightarrow E_k(m) \in \Gamma_A$

Ax6 表示:如果 m 和加密密钥 k_{enc} 属于知识集Γ_A,那么采用该密钥加密的消息 $E_k(m)$属于Γ_A.

- Ax7:$E_k(m) \in \Gamma_A \wedge k_{dec} \in \Gamma_A \wedge k_{dec} \equiv k \rightarrow m \in \Gamma_A$

Ax7 表示:如果加密消息 $E_k(m)$和相应的解密密钥 k_{dec} 属于知识集Γ_A,那么密文 m 属于Γ_A.

- Ax8:$m \in \Gamma_A \wedge k_{x \cdot sig} \in \Gamma_A \rightarrow S_{k \cdot x}(m) \in \Gamma_A$

Ax8 表示:如果 m 和任一实体 x 的签名密钥 $k_{x \cdot sig}$ 属于知识集Γ_A,那么 x 对 m 的签名消息 $S_{k \cdot x}(m)$属于Γ_A.

- Ax9:$S_{k \cdot x}(m) \in \Gamma_A \wedge m \in \Gamma_A \wedge k_{x \cdot ver} \in \Gamma_A \wedge A \propto S_{k \cdot x}(m) \rightarrow A \succ (x \triangleright m)$

Ax9 表示:如果签名消息 $S_{k \cdot x}(m)$、被签名消息 m 和对应的签名验证密钥 $k_{x \cdot ver}$ 属于知识集Γ_A,且 A 验证签名正确,那么 A 相信 x 发送了 m.这里,有一个隐含的事实是:如果 x 发送了 m,那么 x 对 m 的有效性负责.

- Ax10:$A \succ (B \triangleright m) \wedge B \in TTP \rightarrow A \succ m$

Ax10 表示:如果 A 相信 B 发送了 m,且 B 是一个可信的第三方实体,那么 A 相信 m 有效.

2.2.3 逻辑描述和正确性证明

FES 逻辑是命题、状态和参与者的有限集合组合,每一个参与者 $P_i \in \{P_1,P_2,\ldots,P_n\}$产生一个本地状态 s_i,一个全局状态用一个 n-元组表示,是所有 n 个参与者本地状态的集合.协议的一次运行是 FES 系统全局状态的一个有限序列,用离散的整数时间参数 t 排序,t=0 表示初始状态.每个参与者的本地状态包括本地进程的状态和拥有的知识集.参与者 P_i 的知识集用Γ_{Pi} 表示,表示在当前 P_i 的所有消息集合,包括初始已知消息、在协议运行中接收的消息和根据已有消息可计算的消息(根据定义 9,且受到计算复杂性理论限制).

定理 2. 如果$\Phi \rightarrow \gamma$,那么对于$\forall s_t \models \Phi | s_t \models \gamma$.

定理 2 表明,对于可由命题集Φ推出的命题γ,在所有使得Φ中命题为真的状态 s 下γ为真.即在协议分析中,当初始假设集合(Φ)为真的情况下,可由该假设集和推理公理推断协议结果(γ),那么该结果是成立的.

证明:假设原子命题集 Ψ_{AP} 为真,下面证明每一推理公理的正确性.

首先考虑 Ax1 和 Ax2,它们的正确性可由接收消息和产生消息的定义直接推出;其次考察公理 Ax3~Ax8,其正确性可由定义 9 和相关真值条件直接推出;Ax9,假设 $s_t \models (S_{k \cdot x}(m) \in \Gamma_A \wedge m \in \Gamma_A \wedge k_{x \cdot ver} \in \Gamma_A)$,且 A 验证签名 $S_{k \cdot x}(m)$是正确的,则必然存在 $s_{t'|0 \le t' \le t} \models x \triangleright m$(根据签名不可仿冒性假设).基于签名性质,可判定:在状态 $s_{t'}$下 x 对 m 的有效性负责.根据信任命题($X \succ \varphi$)及其真值条件,有 $s_t \models A \succ (x \triangleright m)$;公理 Ax10 的正确性基于可信第三方的定义[24],即如果 TTP 发送了 m(这里隐含了 TTP 确认 m 有效的事实),那么 A 相信 m 有效.

由前面的分析可知推理公理是正确的,如果可根据推理公理由命题集Φ推导γ,那么在使得Φ中所有命题为真的所有状态下,γ为真. □

3 案例分析

Pagnia 等人提出用协议子模块组合的方式实现不同层次的公平性[5].根据实体的不同需求,各子模块间可相互组合构成不同的交换协议.Pagnia 等人认为,全部 5 个子模块的组合协议(记为 PVG 交换协议)可实现强公

平性(strong fairness).但是采用本文方法分析发现,针对 PVG 交换协议存在两种攻击方案.

PVG 交换协议主要有商品购买者(*C*)、商品提供者(*V*)和可信第三方(*T*)等 3 种实体,分为 5 个子协议模,如图 2 所示.模块 1 负责协商产品和支付以及选择可信第三方 *T*.模块 2 为交换准备阶段,由 *V* 向 *C* 发送加密数字商品 *EP*、用 *T* 的公钥加密的商品解密密钥 R_T 和不可否认证据 S_V,*C* 验证 S_V 并选择继续还是放弃交换.模块 3 实现支付和解密密钥的交换,如果双方实体诚实且无信道错误,那么双方成功交换且协议到此结束;否则,*C* 可选择启用模块 4 进行争端解决.在模块 4 中,*T* 验证证据 S_V,检查并保存支付,解密 R_T 并将 *R* 发送给 *C*;然后,*C* 解密数字商品并验证是否符合其描述,如果符合描述则协议成功结束;否则,*C* 可启用模块 5,请求 *T* 验证加密数字商品的正确性.如果 *T* 证实数字商品不符合其描述,那么 *T* 撤销支付.大多数情况下,在模块 4 即可重建公平性,且负载更低.

Module 1: $C\rightarrow V$: $desc_{prod}$, T
$V\rightarrow C$: $desc_{pay}$, T
Module 2: $C\rightarrow V$: *order_product*
$V\rightarrow C$: S_V, EP, R_T
Module 3: $C\rightarrow V$: *payment*
$V\rightarrow C$: R
Module 4: $C\rightarrow T$: $desc_{prod}$, $desc_{pay}$, *payment*, H, R_T, S_V
$T\rightarrow C$: R
Module 5: $C\rightarrow T$: *payment*, $desc_{prod}$, $desc_{pay}$, T, EP, R_T, S_V
$T\rightarrow C$: R or *T revoke payment*

Fig.2 PVG fair exchange

图 2 PVG 公平交换协议

3.1 PVG协议形式化分析

定义 13. PVG 协议由五元组$\Sigma_{PVG}=\langle \Pi,\Psi,\Im,\sigma,\rho\rangle$表示,其初始状态定义为 $s_0=\langle X,\varepsilon_0,\Gamma_0,t_0\rangle$:

- $X\in\{C,V,T,I\}$;$\varepsilon_{X\cdot 0}=Ini$;$t_0=0$;
- $\Gamma_{C\cdot 0}=\{\Pi_{C\cdot 0}=\{C,V,T\},M_{C\cdot 0}=\{desc_{prod},pay\},K_{C\cdot 0}=\{K_{X\cdot ver}\}\}$;
- $\Gamma_{V\cdot 0}=\{\Pi_{V\cdot 0}=\{V\},M_{V\cdot 0}=\{desc_{pay},pro\},K_{V\cdot 0}=\{K_{Xenc},k_{Vsig}\}\}$;
- $\Gamma_{T\cdot 0}=\{\Pi_{T\cdot 0}=\{T\},M_{T\cdot 0}=\varnothing,K_{T\cdot 0}=\{k_{T\cdot enc},k_{T\cdot dec},K_{X\cdot ver}\}\}$;
- $\Gamma_{I\cdot 0}=\{\Pi_{I\cdot 0}=\{I\},M_{I\cdot 0}=\varnothing,K_{I\cdot 0}=\{K_{I\cdot dec},K_{I\cdot sig},K_{X\cdot ver},K_{X\cdot enc}\}\}$.

协议的初始状态描述了各参与者进程在协议开始时的状态和所拥有的知识.其中,*I* 表示某一个(或多个)攻击者.*I* 的初始消息集合为空,初始密钥集包括他自己的私钥(用于解密和签名的密钥)和所有参与者的公钥(包括用于加密和签名验证的密钥).根据本文模型(见第 2.1 节),*I* 可以通过与不诚实的参与者 *C* 或 *V* 合谋对协议进行攻击,将 *I* 与 *C* 的合谋记为 I_C,I_C 的初始知识集$\Gamma_{Ic\cdot 0}=\Gamma_{C\cdot 0}\cup\Gamma_{I\cdot 0}$.反之,*I* 与 *V* 的合谋与此类似.同时,假定 *T* 是诚实的且不与 *C* 或 *V* 合谋,即 $T\notin I$(文中将 *order_product* 简写为 *ord*,*payment* 简写为 *pay* 以及 *product* 简写为 *pro*).

PVG 协议有效性易得到验证.当 *C* 和 *V* 都诚实的情况下(采用攻击者模型(a),见第 2.1 节),即使在模块 3 中有消息丢失,在 *T* 的帮助下,*C* 和 *V* 也都能获得他们期望的消息.本文重点是分析协议的公平性和时限性,即存在不诚实实体的情况下,协议是否能够确保交换双方的公平.下面分别从 *C* 不诚实和 *V* 不诚实两个方面来分析.

3.1.1 PVG 协议攻击方案 1

首先,假设实体 *C* 不诚实,*V* 诚实,*C* 和 *I* 合谋(记为 I_C)对协议进行攻击,有 $V\notin I_C\wedge T\notin I_C$.$I_C$ 的目标是在不付出 *payment* 的情况下获得有效的 *product*.本文采用模型检测的思想,检验是否存在一条路径使得 I_C 能够实现这一目标.

定理 3. 当模块 2 结束时(记为时刻 $i\in\{1,2,\ldots,n\}$),PVG 协议的状态为 $s_i=\langle X,\varepsilon_i,\Gamma_i,i\rangle$:

- $X\in\{I_C,V,T\}$;$\varepsilon_{Ic\cdot i}=Act$,$\varepsilon_{V\cdot i}=Wai$,$\varepsilon_{T\cdot i}=Ini$;
- $\Gamma_{Ic\cdot i}=\{\Pi_{Ic\cdot i}=\{I_C,V,T\},M_{Ic\cdot i}=\{desc_{prod},desc_{pay},EP,H,R_T,ord,S_V,pay\},K_{Ic\cdot i}=\{k_{I\cdot dec},k_{I\cdot sig},K_{X\cdot ver},K_{X\cdot enc}\}\}$;

- $\Gamma_{V\cdot i}=\{\Pi_{V\cdot i}=\{C,V,T\},M_{V\cdot i}=\{desc_{prod},desc_{pay},EP,H,ord,R_T,S_V,pro\},K_{V\cdot i}=\{R,K_{X\cdot enc},k_{V\cdot sig}\}\}$;
- $\Gamma_{T\cdot i}=\{\Pi_{T\cdot i}=\{T\},M_{T\cdot i}=\varnothing,K_{T\cdot i}=\{k_{T\cdot enc},k_{T\cdot dec},K_{X\cdot ver}\}\}$.

证明:定理 3 可由如下推理得到:

$t_{Ic}=1: I_C \triangleright desc_{prod} \,\|\, T \Rightarrow \varepsilon_{Ic\cdot 1}=Wai \wedge \oplus Timer_{Ic}$.

$t_V=1: V \triangleleft desc_{prod} \,\|\, T \Rightarrow \varepsilon_{V\cdot 1}=Act \wedge (desc_{prod},T,C)\in \Gamma_V$.

$t_V=2: V \triangleright des_{pay} \,\|\, T \Rightarrow \varepsilon_{V\cdot 2}=Wai \wedge \oplus Timer_V$.

$t_{Ic}=2: (\Diamond Timer_{Ic} \Rightarrow \varepsilon^*_{Ic\cdot 2}=Abo) \vee (I_C \triangleleft desc_{pay} \,\|\, T \Rightarrow \varepsilon_{Ic\cdot 2}=Act \wedge \otimes Timer_{Ic} \wedge desc_{prod}\in \Gamma_{Ic})$.

$t_{Ic}=3: I_C \ni \wedge \triangleright ord \Rightarrow \varepsilon_{Ic\cdot 3}=Wait \wedge \oplus Timer_{Ic} \wedge ord \in \Gamma_{Ic}$.

$t_V=3: (\Diamond Timer_V \Rightarrow \varepsilon^*_{V\cdot 3}=Abo) \vee (V \triangleleft ord \Rightarrow \varepsilon_{V\cdot 3}=Act \wedge \otimes Timer_V \wedge ord \in \Gamma_V)$.

$t_V=4: V \ni (R,S_V,EP,R_T) \wedge V \triangleright S_V \,\|\, EP \,\|\, R_T \Rightarrow \varepsilon_{V\cdot 4}=Wai \wedge \oplus Timer_V \wedge (R,S_V,EP,R_T)\in \Gamma_V$.

$t_{Ic}=4: (\Diamond Timer_{Ic} \Rightarrow \varepsilon^*_{Ic\cdot 4}=Abo) \vee (I_C \triangleleft S_V \,\|\, EP \,\|\, R_T \wedge I_C \propto S_V \Rightarrow \varepsilon_{Ic\cdot 4}=Act \wedge \otimes Timer_V \wedge (S_V,EP,R_T)\in \Gamma_{Ic})$.

此时可得$\varepsilon_{Ic\cdot i}=\varepsilon_{Ic\cdot 4},\varepsilon_{V\cdot i}=\varepsilon_{V\cdot 4}$,各个参与者的知识集由初始集合加上接收和产生的新消息组成.由于 T 并没有参与这一阶段协议,所以维持初始状态.另外,$\varepsilon^*_{Ic\cdot 2},\varepsilon^*_{Ic\cdot 3},\varepsilon^*_{V\cdot 3}$ 也是可能出现的结束状态.由于不揭示协议的任何性质,这里忽略这些状态. □

本文的推理过程采用了类似 SVO 逻辑[13]的表示方法,应用了第 2.2.2 节中定义的推理公理.例如,在 t_V=1 步骤中应用了公理 Ax1 和 Ax3,其余类似.但是,新逻辑扩展了实体状态的转移过程,为了能够更好地理解推理过程,图 3 演示了定理 3 中 I_C 的状态演化过程.其中,*Event* 表示发生的事件.

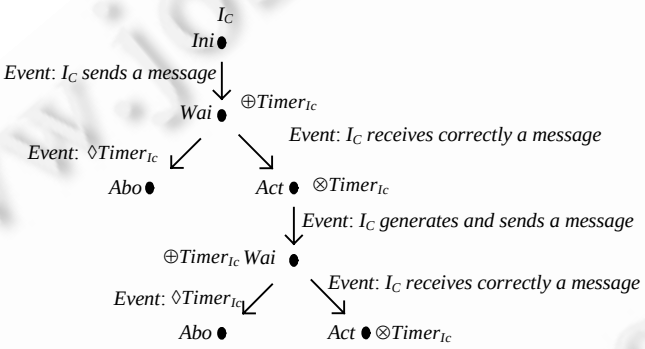


Fig.3 An instantiation of state transformations

图 3 状态转移实例

定理 4. 当模块 4 结束时(记为时刻 $l\in\{1,2,\ldots,n\}$),PVG 协议的状态为 $s_l=\langle X,\varepsilon_l,\Gamma_l,l\rangle$:

- $X\in\{I_C,V,T\}$;$\varepsilon_{Ic\cdot l}=Suc,\varepsilon_{V\cdot l}=Abo,\varepsilon_{T\cdot l}=Suc$;
- $\Gamma_{Ic\cdot l}=\{\Pi_{Ic\cdot l}=\{I_C,V,T\},M_{Ic\cdot l}=\{desc_{prod},desc_{pay},desc^*_{pay},ord,EP,H,R_T,S_V,desc^*_{pay},pay^*,R,pro\}$,
  $K_{Ic\cdot l}=\{k_{I\cdot dec},k_{I\cdot sig},K_{X\cdot ver},K_{X\cdot enc}\}\}$;
- $\Gamma_{V\cdot l}=\{\Pi_{V\cdot l}=\{C,V,T\},M_{V\cdot l}=\{desc_{prod},desc_{pay},EP,H,ord,R_T,S_V,pro\},K_{V\cdot l}=\{R,K_{X\cdot enc},k_{V\cdot sig}\}\}$;
- $\Gamma_{T\cdot l}=\{\Pi_{T\cdot l}=\{C,I_C,T\},M_{T\cdot l}=\{desc_{prod},desc^*_{pay},H,R_T,S^*_{Ic},pay^*\},K_{T\cdot l}=\{k_{T\cdot enc},k_{T\cdot dec},K_{X\cdot ver},R\}\}$.

证明:当模块 2 结束时,I_C 可选择进入模块 3 或模块 4.I_C 为了不付出 *payment*,因此跳过模块 3 直接进入模块 4.由推理可得:

$t_{Ic}=5: I_C \ni (desc^*_{pay}, S^*_{Ic}) \wedge I_C \rhd desc_{prod} \| desc^*_{pay} \| pay^* \| H \| R_T \| S^*_{Ic} \Rightarrow \varepsilon_{Ic\cdot 5}=Wai \wedge \oplus Timer_{Ic} \wedge (desc^*_{pay}, S^*_{Ic}) \in \Gamma_{Ic}.$

$t_T=1: T \lhd desc_{prod} \| desc^*_{pay} \| pay^* \| H \| R_T \| S^*_{Ic} \wedge T \propto pay^* \wedge T \propto (desc^*_{pay}=f(pay^*)) \wedge T \propto S^*_{Ic} \Rightarrow$

$\varepsilon_{T\cdot 1}=Act \wedge T \succ (I_C \rhd S^*_{Ic}) \wedge (desc_{prod}, desc^*_{pay}, pay^*, R_T, S^*_{Ic}) \in \Gamma_T.$

$t_T=2: T \ni \wedge \rhd R \Rightarrow \varepsilon_{T\cdot 2}=Suc \wedge R \in \Gamma_T.$

$t_{Ic}=6: (\Diamond Timer_{Ic} \Rightarrow \varepsilon^*_{Ic\cdot 6}=Abo) \vee (I_C \lhd R \Rightarrow \varepsilon_{Ic\cdot 6}=Act \wedge \otimes Timer_V \wedge R \in \Gamma_{Ic}).$

$t_{Ic}=7: I_C \ni pro \Rightarrow pro \in \Gamma_{Ic} \wedge \varepsilon_{Ic\cdot 7}=Suc.$

$t_V=5: \Diamond Timer_V \Rightarrow \varepsilon_{V\cdot 5}=Abo.$

此时可得$\varepsilon_{Ic\cdot l}=\varepsilon_{Ic\cdot 7}$,$\varepsilon_{V\cdot l}=\varepsilon_{V\cdot 5}$,$\varepsilon_{T\cdot l}=\varepsilon_{T\cdot 2}$.$I_C$利用$T$获得有效的产品,而$V$在等待一定时间后终止交换,且并未发现自身利益受到了侵害.其中,$S^*_{Ic}=S_{K\cdot I}(desc_{prod}, desc^*_{pay}, T, H, R_T)$为攻击者$I$产生的伪造签名.另外,$\varepsilon^*_{Ic\cdot 6}$也是可达的结束状态.这里忽略这一状态,因为不诚实的实体I_C不会主动终止协议运行. □

由于篇幅原因,在定理 4 的分析过程中,本文省略了C进入模块 3 的运行分支.

定理 5. 如果C不诚实,且存在实体$I \notin \{V,T\}$与C合谋,那么 PVG 交换协议不具有公平性和时限性.

证明:定理 5 可由定理 3 和定理 4 直接推出.由定理 4 可知,C与$I \notin \{V,T\}$合谋,可获得正确的数字商品($pro \in \Gamma_{Ic}$),而V在长时间等待后选择放弃,没能获得有效支付($pay \notin \Gamma_V$).这与公平性和时限性的定义相悖. □

图 4 采用串空间模型[26]的图形表示方式描述这种攻击方案.

形成这种攻击的缺陷在于被签名项($desc_{prod}$,$desc_{pay}$,T,H,R_T)与签名者V之间没有建立牢固的对应关系,使得攻击者存在伪造签名的可能性.为了弥补这个缺陷,需要修改$R_T=E_{k\cdot t}(R \| S_{k\cdot v}(R))$.由于在$t_{Ic}=5$之前$R \notin \Gamma_{Ic}$,且$I_C$伪造$R^* \neq R$没有意义,那么$I_C$不能伪造$R_T$.这样,在上述攻击场景下,$T$可以验证对$R$的签名者($V$)与对$S^*_{Ic}$的签名者($I$)不是同一实体,那么$T$会直接终止交换,而不会发送密钥$R$给$C$.

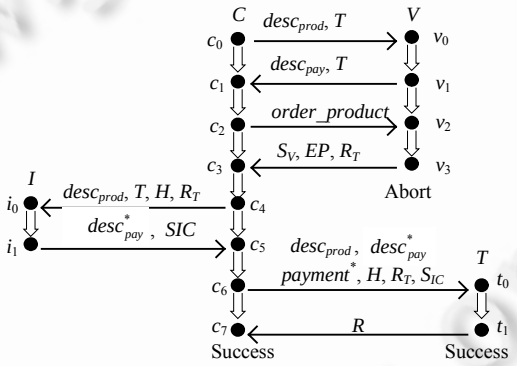


Fig.4 An attack on the PVG protocol

图 4 PVG 协议的一种攻击方案

3.1.2 PVG 协议攻击方案 2

另一方面,假设V不诚实而C诚实,V可与$I \notin \{C,T\}$合谋(记为I_V).I_V的目标是不付出正确产品的情况下获得有效的支付.

定理 6. 当模块 4 结束时(记为时刻$j \in \{1,2,\ldots,n\}$),PVG 协议的状态为$s_j=\langle X, \varepsilon_j, \Gamma_j, j\rangle$:

- $X \in \{C, I_V, T\}$;$\varepsilon_{C\cdot j}=Act$,$\varepsilon_{Iv\cdot j}=Suc$,$\varepsilon_{T\cdot j}=Suc$;
- $\Gamma_{C\cdot j}=\{\Pi_{C\cdot j}=\{C,V,T\}, M_{C\cdot j}=\{desc_{prod}, desc_{pay}, EP, H, R_T, ord, S_V, pay, pro^*\}, K_{C\cdot j}=\{R, K_{X\cdot ver}\}\}$;
- $\Gamma_{Iv\cdot j}=\{\Pi_{Iv\cdot j}=\{C,I_V,T\}, M_{Iv\cdot j}=\{desc_{prod}, desc_{pay}, EP, H, ord, R_T, S_V, pro^*, pro, pay\}$,
  $K_{Iv\cdot j}=\{R, k_{I\cdot dec}, k_{I\cdot sig}, K_{X\cdot ver}, K_{X\cdot enc}, k_{V\cdot sig}\}\}$;
- $\Gamma_{T\cdot j}=\{\Pi_{T\cdot j}=\{C,V,T\}, M_{T\cdot j}=\{desc_{prod}, desc_{pay}, H, R_T, S_V, pay\}, K_{T\cdot j}=\{k_{T\cdot enc}, k_{T\cdot dec}, K_{X\cdot ver}, R\}\}$.

证明:定理 6 的证明过程与定理 3 和定理 4 类似,这里略. □

此时有 $pro^* \neq pro$,即有效的 $pro \notin \Gamma_C$.但 $pay \in \Gamma_{Iv}$,那么 C 必然会启用模块 5.协议的公平性依赖于 pay 是否可撤销.

定理 7. 假设 V 不诚实,且存在实体 $I \notin \{C,T\}$ 与 V 合谋,那么 PVG 交换协议不能重建公平性.

证明:定理 7 可由如下推理得到:

$$t_C = j+1 : C \rhd desc_{prod} \| desc_{pay} \| pay \| T \| EP \| R_T \| S_V \Rightarrow \varepsilon_{C \cdot l} = Abo.$$

$$t_T = 1 : T \lhd desc_{prod} \| desc_{pay} \| pay \| T \| EP \| R_T \| S_V \wedge T \propto pay \wedge T \propto (desc_{pay} = f(pay)) \wedge T \propto S_V \Rightarrow$$
$$\varepsilon_{T \cdot 1} = Act \wedge (desc_{prod}, desc_{pay}, pay, EP, R_T, S_V) \in \Gamma_T.$$

$$t_T = 2 : (T \ni pro^* \wedge T \propto (desc_{prod} \neq f(pro^*)) \wedge \perp pay \Rightarrow \varepsilon^*_{T \cdot 2} = Suc) \vee$$
$$(T \ni pro^* \wedge T \propto (desc_{prod} \neq f(pro^*)) \wedge \neg \perp pay \Rightarrow \varepsilon_{T \cdot 2} = Abo).$$

支付 pay 是时间敏感消息,是否可撤销取决于消息最终到达 T 的时间.如果弱 DV 攻击者 I 延迟消息,使得消息到达 T 时 pay 已经无效($\neg \perp pay$,即 V 已兑现支付),那么 T 不能通过撤销支付来重建公平性,而需要使用外部的争端裁决机制,如法律等手段. □

Pagnia 假设 T 具有强撤销支付能力,即任何时候支付可撤销.这一假设显然不符合现实情况.在实际的电子商务环境中,支付只能是在一定的时间段内可撤销.形成这种漏洞的原因是:协议不满足一致性(见第 1 节).有两种手段可弥补 PVG 协议的这一缺陷:一是在 C 与 T 之间建立无时延的信道,即保证消息在确定时间内到达指定实体,这在实际应用中实施起来是比较困难的;另一种方法是使得数字商品的真伪在交换前可验证,即实现一致性验证,这可通过第三方权威机构为数字商品颁发数字证书的方法来实现,如 Bao[3]和 Ray[4]等人的解决方案.

4 分析与比较

目前,已有许多公平交换协议的形式化分析方法.SVO 逻辑[13]是一种重要的、基于信任逻辑的方法.Zhou 等人首先采用 SVO 逻辑分析不可否认协议[12],但是韩志耕等人[23]研究指出,SVO 逻辑难以分析协议的时限性,他们通过添加时间演算过程改进了这一缺陷.不过到目前为止,还没有见到采用 SVO 逻辑方法成功分析乐观型公平交换协议的成功案例,主要原因有以下两点:第一,攻击者模型不同.SVO 逻辑采用经典 DV 模型,未区分可恢复信道与不可靠信道.另外,SVO 逻辑总是假定认证双方是诚实的,不考虑不诚实实体的内部攻击行为.本文定义了乐观协议的新攻击者模型,将信道问题进行转化,并区分参与者的行为属性;第二,公平性目标难以用 SVO 逻辑语言描述.由于乐观协议具有多个分支,且存在多种可能的执行结果,其最终目标难以用 SVO 逻辑语言简洁描述.对此,本文将协议定义为随时间演化的系统,采用模型检查的思想验证协议所有运行状态,避免了为协议运行实例预先设定结束状态的问题.

文献[21]使用 Z 语言规范作为描述工具,构造了一个新的公平交换协议形式化模型.该模型定义了事件和时序关系,定义了公平性和不可滥用性等公平交换协议应具有的性质,通过求精化过程推出协议的形式化结构模型.文献[21]也考虑了参与者的行为属性和信道问题,但是与本文的攻击者模型相反,该模型将参与者的不诚实行为归结于交换双方之间的不可靠信道,提出了“消息影子”这一概念描述接收方未能及时准确地接收消息的事件.但是,该模型未考虑外部攻击者与不诚实参与者的共谋.在真实世界应用中,通常外部攻击者比诚实参与者拥有更多资源和技术,拥有更强的计算能力.因此,考虑外部攻击者的作用是必要的.本文的案例分析(见第 3.1.1 节)也例证了这一必要性,这也是本文模型的主要贡献之一.

与现有同类方法比较,本文方法主要有以下特点:首先,把协议实体看作异步网络环境下具有本地存储和处理能力的通信进程,降低了协议分析的抽象层次,使得协议的形式化描述更加符合应用实际;其次,在模型层面区分参与者的行为属性,使得协议分析更具有针对性;第三,引入弱 DV 攻击者来描述可恢复信道,将不诚实参与者与外部攻击者的共谋归结为 DV 攻击者,这在现有研究中未发现相同的成功实例;第四,第一次定义了电子项的认证属性,案例分析表明,这一属性是必要的.另外,本文逻辑来源于经典的BAN类信任逻辑,去除了BAN逻辑中关于实体认证的逻辑公式,增加了时序控制、消息有效性验证等逻辑描述,传承了 BAN 类逻辑简单易用的优

点,并且结合图形描述工具给出了攻击发生时系统运行的过程.

5 结束语

本文在详细分析公平交换协议应具有的各项属性的基础上,定义了交换协议中电子项的认证属性,提出了乐观协议分析的 3 类攻击者模型.模型将信道错误对应于攻击者的行为,将不诚实实体和入侵者的共谋归结为入侵者的行为.在此模型下,本文定义了融合 BAN 类逻辑思想的知识推理逻辑,新逻辑定义了实体行为公式和密码学计算原语,引入了离散时间序列和时间算子控制协议状态转换以及状态之间的时序关系,并给出了新逻辑的正确性条件.案例分析表明,新的推理逻辑能用于分析交换协议的公平性和时限性.另外,本文还揭示了针对协议实例的两种攻击方案及其形成的原因.这两种攻击方案表明了该协议不具有其作者宣称的强公平性,且第 2 种攻击的形成原因正是由于协议不满足本文定义的消息项一致性.就我们掌握的资料显示,针对该协议的这两种攻击方案是由本文首次提出.

尽管取得了一些成果,本文工作还并不完善,我们期望从以下方面继续开展研究工作:第一,本文方法的有效性还有待进一步地广泛验证;第二,使用本文的方法进行公平交换协议分析要求研究人员具有深厚的相关理论知识,实现基于本文逻辑方法和模型检查理论的自动推理技术还有待进一步研究;第三,多方的公平交换问题正逐渐成为该领域的研究热点,本文的形式化模型易于扩展为多方实体共谋的情形,这还有待进一步研究.

致谢 在此,我们向对本文的工作给予支持和建议的专家和同行表示感谢.

References:

[1] Asokan N. Fairness in electronic commerce [Ph.D. Thesis]. Waterloo: University of Waterloo, 1998.

[2] Asokan N, Shoup V, Waidner M. Asynchronous protocols for optimistic fair exchange. In: Proc. of the IEEE Symp. on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1998. 86−99.

[3] Bao F, Deng RH, Mao W. Efficient and practical fair exchange protocols with off-line TTP. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 1998. 77−85. [doi: 10.1109/SECPRI.1998.674825]

[4] Ray I, Ray I, Natarajan N. An anonymous and failure resilient fair-exchange e-commerce protocol. Decision Support Systems, 2005, 39(3):267−292. [doi: 10.1016/j.dss.2003.10.011]

[5] Pagnia H, Vogt H, Gärtner FC. Fair exchange. The Computer Journal, 2003,46(1):55−76. [doi: 10.1093/comjnl/46.1.55]

[6] Wang H, Guo H, Lin M, Yin J, He Q, Zhang J. A new dependable exchange protocol. Computer Communications, 2006,29(10): 2770−2780. [doi: 10.1016/j.comcom.2005.10.028]

[7] Hernandez-Ardieta JL, Gonzalez-Tablas AI, Alvarez BR. An optimistic fair exchange protocol based on signature policies. Computers & Security, 2008,27(10):309−322. [doi: 10.1016/j.cose.2008.07.005]

[8] Kremer S, Markowitch O. Optimistic non-repudiable information exchange. In: Biemond J, ed. Proc. of the 21st Symp. on Information Theory in the Benelux. Wassenaar: Werkgemeenschap Informatie-en Communicatietheorie, 2000. 139−146.

[9] Zhou J, Gollmann D. An efficient non-repudiation protocol. In: Proc. of the 10th IEEE Computer Security Foundations Workshop. IEEE Computer Society Press, 1997. 126−132. [doi: 10.1109/CSFW.1997.596801].

[10] Kailar R. Accountability in electronic commerce protocols. IEEE Trans. on Software Engineering, 1996,22(5):313−328. [doi: 10.1109/32.502224]

[11] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990,8(1):18−36. [doi: 10.1145/77648.77649]

[12] Zhou J, Gollmann D. Towards verification of non-repudiation protocols. In: Proc. of the Int'l Refinement Workshop and Formal Methods Pacific. Canberra: Springer-Verlag, 1998. 370−380.

[13] Syverson PF, Van Oorschot PC. A unified cryptographic protocol logic. NRL Publication 5540-227. Washington: Naval Research Laboratory, 1996.

[14] Schneider S. Formal analysis of a non-repudiation protocol. In: Proc. of the 11th IEEE Computer Security Foundations Workshop. Washington-Brussels-Tokyo: IEEE Computer Security Press, 1998. 54−65. [doi: 10.1109/CSFW.1998.683155]

[15] Bella G, Paulson LC. Accountability protocols: Formalized and verified. ACM Trans. on Information System Security, 2006,9(2): 138−161. [doi: 10.1145/1151414.1151416]

[16] Zhou J, Gollmann D. A fair non-repudiation protocol. In: Proc. of the IEEE Symp. on Research in Security and Privacy, Research in Security and Privacy. IEEE Computer Security Press, 1996. 55−61. [doi: 10.1109/SECPRI.1996.502669]

[17] Shmatikov V, Mitchell JC. Finite-State analysis of two contract signing protocols. Theoretical Computer Science, 2002,283(2): 419−450. [doi: 10.1016/S0304-3975(01)00141-4]

[18] Garay JA, Jakobsson M, MacKenzie P. Abuse-Free optimistic contract signing. In: Proc. of the Advance in Cryptology-Crypto'99. LNCS 1666, Berlin, Heidelberg: Springer-Verlag, 1999. 449−466.

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

[20] Dashti MT. Keeping fairness alive [Ph.D. Thesis]. Geboren te Kordkoy: Vrije Universiteit Amsterdam, 2008.

[21] Qing SH, Li GC. A formal model of fair exchange protocols. Science in China Ser. F: Information Sciences, 2005,48(4):499−512.

[22] Dolev D, Yao AC. On the security of public key protocols. IEEE Trans. on Information Theory, 1983,29(2):198−208. [doi: 10.1109/TIT.1983.1056650]

[23] Li BT, Luo JZ. Formal analysis of timeliness in non-repudiation protocols. Journal of Software, 2006,17(7):1510−1516 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1510.htm [doi: 10.1360/jos171510]

[24] Qing SH. TTP roles in electronic commerce protocols. Journal of Software, 2003,14(11):1936−1943 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1936.htm

[25] Pagnia H, Gärtner F. On the impossibility of fair exchange without a trusted third party. Technical Report, TUD-BS-1999-02, Darmstadt: Darmstadt University of Technology, 1999.

[26] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999,7(2-3): 191−230.

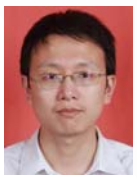
附中文参考文献:

[23] 黎波涛,罗军舟.不可否认协议时限性的形式化分析.软件学报,2006,17(7):1510−1516. http://www.jos.org.cn/1000-9825/17/1510.htm [doi: 10.1360/jos171510]

[24] 卿斯汉.电子商务协议中的可信第三方角色.软件学报,2003,14(11):1936−1943. http://www.jos.org.cn/1000-9825/14/1936.htm

陈明(1978－),男,重庆人,博士生,主要研究领域为形式化分析技术,分布式计算.

吴开贵(1966－),男,博士,副教授,CCF 会员,主要研究领域为信息安全,分布式计算.



吴长泽(1980－),男,博士,讲师,主要研究领域为网格计算,容错计算.

徐洁(1963－),男,博士,教授,博士生导师,主要研究领域为分布式系统,网络计算.

吴中福(1938－),男,教授,博士生导师,CCF 会员,主要研究领域为计算机网络与通信,现代远程教育技术.