

## 基于离线可信第三方的电子支付协议公平性分析

田树华,陈立佳,李建茹

(唐山学院 信息工程系,河北 唐山 063020)

(chz2000@yahoo.cn)

**摘要:**基于离线可信第三方的电子支付协议通常具有复杂结构,它由多个子协议组合而成,与传统认证协议有显著差别,主要表现在协议目标和攻击者模型两个方面。电子支付协议最主要目的是实现买卖双方的公平交换,同时假定交换双方都可能是不诚实的,需要考虑来自协议合法实体的内部攻击。在重新定义协议公平性和攻击者模型的基础上,提出扩展的串空间模型,以一个真实的电子支付协议为对象,演示了基于串空间理论电子支付协议公平性形式化模型和分析方法,并指出该协议存在安全缺陷,提出改进意见。

**关键词:**电子支付协议;离线可信第三方;公平性;串空间

**中图分类号:** TP309 **文献标志码:** A

## Fairness analysis of electronic payment protocol based on offline TTP

TIAN Shu-hua, CHEN Li-jia, LI Jian-ru

(Department of Information Engineering, Tangshan College, Tangshan Hebei 063020, China)

**Abstract:** The electronic payment protocol based on offline TTP is made up of multiple sub-protocols, and is significantly different from traditional authentication protocol, especially on protocol goal and penetrator model. The main purpose of the electronic payment protocol is to realize fair exchange between buyers and sellers who are assumed to be dishonest. Then, it is necessary for those buyers and sellers to prevent the internal attack. On the basis of redefining protocol fairness and penetrator model, an extended strand space model which took an electronic payment protocol as object was proposed to demonstrate a fairness formal analysis method. The security deficiency and improvement suggestions of the electronic payment protocol were also discussed.

**Key words:** electronic payment protocol; offline TTP; fairness; strand space

## 0 引言

随着电子商务的迅猛发展,与之相关的安全问题正日显突出。在电子商务协议中,保护交易双方免受内部攻击与保护其不受外来攻击同样重要。因此,除了数据完整性和机密性等传统安全问题外,交易中的公平性问题同样值得重视。一般来说,公平交换问题就是关于协议参与者交换有价值数据的问题,其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。而电子支付协议是一种特定的公平交换问题,其目的是在购买者和商家之间交换数字商品和付款凭证,保护客户、商家彼此互不欺骗,公平完成商业交易。

串空间模型<sup>[1-2]</sup>是在 1999 年提出的安全协议分析模型,它借助带有因果关系的有向图来描述协议的执行过程。协议主体的行为序列构成串,而串空间则是所有串的集合;不同协议主体的串之间通过消息数据的收发相互关联从而形成串。串空间模型能准确地描述协议执行过程中事件的先后顺序及因果关系,为研究人员提供了一种有效的协议分析理论。本文采用串空间理论进行电子支付协议公平性分析。考虑到串空间理论原本用于分析传统的身份认证协议,而电子支付协议与认证协议存在两个主要的不同:一是协议目标不同,认证协议主要分析认证性,而支付协议主要关注公平性问题;二是协议的攻击者模型不同,认证协议主要考虑来自协议外部的攻击,而支付协议则需要防范与之交易的对方实体的欺骗行

为。基于此,本文扩展了串空间理论,以一种实际的电子支付协议——EMH 协议<sup>[3]</sup>为实例,演示了基于串空间理论电子支付协议公平性形式化模型和分析方法,并指出 EMH 协议存在的安全缺陷,提出改进意见。

## 1 相关研究

### 1.1 交换协议

20 世纪 80 年代,交换协议主要用于在实体间进行秘密信息或数字合同签名交换,这一时期的交换协议都没有可信第三方(Trusted Third Party, TTP)的参与。Pagnina 等人<sup>[4]</sup>认为如果没有可信第三方的参与,交换协议将不能取得公平性。目前,大多数的交换协议都基于可信第三方<sup>[5]</sup>,主要分为四种类型<sup>[5-6]</sup>:Inline TTP、Online TTP、Offline TTP 和 Transparent TTP。在 Inline 模式,TTP 作为交换中介,参与交换实体间每一条信息的传递,这种模式严重依赖 TTP,容易遭受拒绝服务攻击,且增加网络负载。在 Online 模式,TTP 作为协议实体的一方,参与每一轮协议执行的部分消息传递。1997 年,Asokan 等人<sup>[7]</sup>第一次提出了 Offline TTP 的思想,将交换协议分为两个阶段,即交换阶段和争端解决阶段。TTP 并不参与信息交换阶段,当协议正常执行而没有产生争端时,TTP 对交换双方是透明的,而当争端出现时,TTP 进行争端裁决,这种模式的优点是大大降低了对于 TTP 的依赖程度。Transparent TTP 是一种特殊的 Offline TTP 形式,它的提出是为了避免因为网络故

收稿日期:2009-02-05;修回日期:2009-03-23。 基金项目:河北省自然科学基金资助项目(F2007000682)。

作者简介:田树华(1973-),男,河北唐山人,讲师,硕士,主要研究方向:数据库、人工智能软件; 陈立佳(1983-),男,河北唐山人,助理讲师,硕士,主要研究方向:网络信息系统; 李建茹,女,助理讲师,硕士,主要研究方向:网络信息系统。

障产生争端时, TTP 做出针对实体的不良裁决。目前, 基于 Offline TTP 的交换协议得到广泛应用, 因此, 本文的工作主要针对基于 Offline TTP 的电子支付协议。

### 1.2 公平性定义

1985 年, Even<sup>[8]</sup>第一次提出了交换协议的计算公平性概念。随后, Ben-Or<sup>[9]</sup>提出公平性的条件概率模型。对于电子支付协议, 比较有代表性的工作是由 Zhou<sup>[10]</sup>提出的模糊公平性, 其定义如下:

如果一个非否认协议是公平的, 那么, 当协议完成时, 交换双方均获得有效的不可否认证据, 并且, 在协议运行的任何阶段, 其中一方不能获得相对于交易另一方的优势。

该定义将公平性归结为双方行为的不可否认性。随后, Asokan<sup>[11]</sup>提出强公平性和弱公平性定义。弱公平性定义了基于 Offline TTP 电子商务协议的公平性需求, 保证受到损害的诚实参与方能向 TTP 证明他的诚实, 并确保公平性。在随后的工作中, 一种被广泛采纳的公平性定义<sup>[5, 12-13]</sup>如下:

**定义 1** 公平性。当交换协议结束时, 要么所有参与实体均能获得他们期望的信息, 要么没有任何一个实体得到任何信息。

可以看出, 这个定义是从协议运行的最终状态来判定协议的公平性, 具有普适性。

### 1.3 公平交换协议形式化方法相关研究

在国外方面, Kailar<sup>[14]</sup>对 BAN 逻辑进行了扩展, 提出了 Kailar 逻辑方法, 该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。Kailar 逻辑能用于证明电子商务协议的不可否认性, 但不能分析协议的公平性。Kremer<sup>[5]</sup>采用模型检测结合可变时序逻辑的方法分析交换协议的公平性, 但该方法基于对协议的逻辑描述, 缺乏对协议行为的直观描述。Pagnia 则提出了公平交换协议的, 能很好地描述协议模块间的关系, 但不能分析组件内部实体的行为。

国内学者卿斯汉等对电子商务协议形式化分析进行了大量研究<sup>[13, 15]</sup>, 提出了一种新的公平交换协议形式化分析模型<sup>[13]</sup>。白硕等提出用非单调动态逻辑系统 NDL 分析电子商务协议<sup>[16]</sup>, 并已对 SET 的一部分业务流程成功地进行了验证。

以上研究工作大多采用推理逻辑进行交换协议的分析, 普遍缺乏对协议行为的直观描述。沈海峰等人<sup>[17]</sup>在串空间的基础上增加了知识推理逻辑, 并用以分析了 ZC 协议<sup>[10]</sup>, 但该方法主要针对基于 Online 模式的交换协议。王涛等人<sup>[18]</sup>扩展了串空间理论, 讨论了串的条件转移和串同步问题, 采用串空间描述复杂的公平性交换协议, 但缺乏有效分析方法的支撑。本文采用串空间理论分析基于 Offline 模式的电子支付协议公平性, 秉承了串空间模型能直观描述协议执行过程中事件先后顺序及其因果关系的优点, 建立起对复杂交换协议行为过程的图形描述, 并给出了有效的分析方法, 通过实例分析演示了本文方法的有效性。

## 2 EMH 电子支付协议

Alaraj 和 Munro 提出了一种基于 Offline TTP 的电子支付协议——EMH 协议<sup>[3]</sup>, 并声称该协议满足公平性。EMH 协议具有消息负载轻、自动争端解决、较少依赖 TTP 等优点。协议采用 RSA 公开密钥算法和 X.509 公钥证书体系。

### 2.1 标识符号说明

C、M、TTP 和 CB 分别表示购买者、商家、可信第三方和购买者银行。

D: 表示数字商品;

P: 表示买家支付凭证;

Desc: 表示数字产品描述;

$h(X)$ : 表示安全单向散列函数;

$PK_a = (e, n) = n^e$ : 表示实体 a 的 RSA 公钥;

$SK_a = (d, n) = n^d$ : 表示实体 a 的 RSA 私钥;

P-Cert: 表示 CB 发布的支付证书, 包含以下组件: d: 支付描述, 包括支付金额等信息; hp: 支付消息摘要; hep: 经  $PK_a$  加密后的支付消息摘要;  $Sig_{CB}$ : CB 对 P-Cert 的签名;

$Cert_{CT}$ : 表示由 TTP 颁发的 C 与 TTP 共有的公钥证书, 与证书相关的公钥  $PK_{ct}$  与其对应的私钥  $SK_{ct}$  由 C 和 TTP 共享;

$Enc_{PK_a}(X) = \{X\}_{PK_a} = X^e \bmod n = Y$ : 表示用  $PK_a$  对消息 X 的加密, 与之相对应的解密方案为:  $Dec_{PK_a}(Y) = Y^d \bmod n = X$ ;

$Sig_a(X) = \{h(X)\}_{PK_a} = (h(X))^d \bmod n$ : 表示实体 a 对消息 X 的签名;

$X \parallel Y$ : 表示消息连接;

$A \rightarrow B: X$ : 表示实体 A 发送消息 X 给 B。

### 2.2 EMH 协议过程

EMH 协议分为三个阶段, 预交换阶段、交换阶段和争端解决阶段。在预交换阶段, C 获得公钥证书  $Cert_{CT}$  和支付证书 P-Cert。在交换阶段, C 与 M 交换数字产品 D 与支付凭证 P。在争端解决阶段, 当出现争端的情况下, M 向 TTP 提交证据证明自己的诚实。协议过程如下。

1) 预交换阶段。

Mes. 1: TTP  $\rightarrow$  C:  $Cert_{CT}$

Mes. 2: CB  $\rightarrow$  C: P-Cert

2) 交换阶段。

Mes. 3: C  $\rightarrow$  M: Desc  $\parallel \{P\}_{PK_{ct}} \parallel P-Cert \parallel Cert_{CT} \parallel Sig_c(P)$

Mes. 4: M  $\rightarrow$  C:  $\{D\}_{PK_{ct}} \parallel Sig_m(D)$

Mes. 5: C  $\rightarrow$  M:  $SK_{ct}$

3) 争端解决阶段。

Mes. 6: M  $\rightarrow$  TTP: Desc  $\parallel \{P\}_{PK_{ct}} \parallel P-Cert \parallel Cert_{CT} \parallel Sig_c(P) \parallel \{D\}_{PK_{ct}} \parallel Sig_m(D)$

Mes. 7: TTP  $\rightarrow$  C:  $\{D\}_{PK_{ct}} \parallel Sig_m(D)$

Mes. 8: TTP  $\rightarrow$  M:  $SK_{ct}$

可以看出, C 在确认收到 D 之前不会发送支付凭证 P 的解密密钥  $SK_{ct}$ , 以此来确保 C 的公平性; 而 M 可通过向 TTP 提交证据 Mes. 6 来获取支付凭证 P 的解密密钥  $SK_{ct}$ , 以此来确保 M 的公平性。但是, 在阶段 3), 如果有任何一条消息不能到达指定的接收者, 即通信信道是不可靠的<sup>[5]</sup>, 那么协议不能满足公平性。同步信道的假设被认为是不实际的<sup>[5]</sup>, 因此, 我们定义有 TTP 参与的通信信道为弹性信道<sup>[5]</sup>, 即信道上传输的消息能够在有限的时间内到达指定的接收者, 但是这个时间的长短不可预知。弹性信道表明, 消息总是能够到达指定的接收者, 但是, 可能由于网络本身的原因或某个恶意实体有意地延迟了消息到达指定接收者的时间。

## 3 电子支付协议公平性形式化模型

串空间模型结合了定理证明和协议迹, 吸纳了 NRL 协议分析器<sup>[19]</sup>、Schneider 秩函数<sup>[20]</sup>和 Paulson 归纳法<sup>[21]</sup>等思想, 使用节点因果关系的有向图来表示协议的运行轨迹, 能够直观地描述协议运行状态, 是一种有效的安全协议形式化分析方法。因此, 本文采用串空间模型来分析电子支付协议的公平性问题。但是, 电子支付协议并不同于传统的认证协议, 传

统认证协议总是假定合法参与实体都是诚实的,只考虑来自协议外部的未知攻击者行为;而支付协议则假定合法参与实体可能是不诚实的,需要考虑合法参与实体的不诚实行为对交换对端的公平性损害。另外,认证协议关注实体身份的认证性和秘密消息的保密性,而支付协议主要关注交换双方的公平性,且往往要求交换双方是匿名的。

### 3.1 EMH 协议公平性定义

1.2 节公平性的定义有两层涵义:1)当交换双方都诚实地执行支付协议且正确完成时,交换双方均能获得他们所期望的信息,即协议具有有效性;2)交换双方可能是不诚实的,当支付协议在运行的任何阶段出现异常而未正确执行时,交换双方都得不到他所期望的信息。EMH 协议中,交换的双方为购买者 C 和商家 M,所交换的信息是支付凭证 P 和数字商品 D,由此,我们将 EMH 协议公平性定义为有效性和碰撞性。

**定义 2 有效性。**假设 C 和 M 都是诚实的,且 EMH 协议正确完成,那么,如果 C 获得了正确的 D,则 M 获得有效支付 P,反之亦然。

**定义 3 碰撞性。**假设 EMH 协议未正确完成,那么,如果 C 未获得正确的 D,当且仅当 M 未获得有效支付 P,反之亦然。

定义 2 和 3 是对定义 1 的分解。有效性考查当交换双方都诚实地执行协议时,EMH 协议是否能有效实现支付凭证 P 和数字商品 D 之间的交换,如不能实现交换则不满足有效性。碰撞性则要求考虑交换双方可能是不诚实的,那么在 EMH 协议结束时<sup>[12]</sup>,交换的其中一方不能获得更多的有用信息,如果其中一方获得一定的优势,则认为 EMH 协议不满足碰撞性。

### 3.2 攻击者模型的调整

传统认证协议的攻击者行为定义主要基于 Dolev-Yao 模型<sup>[22]</sup>。Dolev-Yao 模型有 3 个显著的特点:1)假定协议所涉及的密码算法是安全的,讨论协议行为的安全性,且协议的安全威胁来自外部的攻击者;二是,假定攻击者有控制信道的能力,即攻击者具有监听、截获、篡改、延迟、发送和阻止消息的能力。交换协议的攻击者行为模型与传统的 Dolev-Yao 模型存在不同,主要表现在两个方面:1)攻击者主要来自协议的内部,即攻击者可能是合法参与协议的任何一方(TTP 除外);2)合法实体在与 TTP 的通信过程中,信道为弹性信道,即攻击者除了不能阻止消息到达指定的接收者外,具有 Dolev-Yao 模型定义的其他能力。

### 3.3 EMH 协议公平性分析

EMH 协议分为三个阶段,在预交换阶段是对交换的准备,不涉及具体的交换过程,因此,我们假定预交换阶段不影响协议的公平性,即只考查交换阶段和争端解决阶段协议的公平性问题。

#### 3.3.1 EMH 协议有效性分析

根据 Pagnia 的组件理论<sup>[12]</sup>,交换协议正确完成,且信息交换成功主要存在两种情况:一是交换阶段顺利完成;二是当交换阶段未能顺利完成出现争端,那么启动争端解决阶段,成功消解争端。EMH 协议定义了由 M 发起的争端解决机制,该协议认为 C 是不需要发起争端解决机制的,因为,按照协议,C 在获得正确的 D 之前是不会将解密密钥发送给 M 的。

在构造交换协议串空间状态图之前,扩展串空间模型中关于协议迹的定义。

**定义 4 边集合。**假设  $\square$  是串空间,集合 S 表示  $\square$  中的

边集合,则  $S = \{\rightarrow, \rightarrow^*, \vdash, \Rightarrow\}$ 。

**定义 5 丢失迹  $\rightarrow^*$ 。**丢失迹  $\rightarrow^*$  是  $\square$  中的一条边,存在节点 n 和 n' 使得  $n \rightarrow^* n'$ ,这里  $\text{term}(n) = +a$ ,而  $\text{term}(n') = \emptyset$ 。

丢失迹描述串空间中消息丢失现象,即消息 a 从节点 n 发出,在传输的过程中由于网络自身因素或是人为干扰,使得 a 未能到达期望的接收节点 n'。这里,“+”表示消息发送,“-”表示消息接收,term(n) 表示节点 n 的消息项。在 3.2 节中,我们定义了交换实体与 TTP 间的通信是弹性信道,但在交换实体之间的通信是在不可靠信道上进行的,存在消息丢失情况,这里消息的丢失可能是人为干扰,也可能是信道自身不可靠引起的。在传统认证协议中,消息的丢失直接导致认证的失败,故没有将消息丢失现象作为特殊情况加以考虑。在交换协议中,某些消息丢失并不一定导致交换失败,所以我们定义丢失迹以扩展串空间理论对消息丢失状态的描述。

**定义 6 延迟迹  $\vdash$ 。**延迟迹  $\vdash$  是  $\square$  中的一条边,存在节点 n、n' 和 m,有  $n \vdash n'$ ,这里  $\text{term}(n) = +a$ ,而  $\text{term}(n') = -a$ ,使得  $n < m < n'$ 。

延迟迹描述攻击者对消息的延迟现象,即消息 a 从节点 n 发出,本来应该在节点 m 前到达某个接收节点 n',但是由于信道原因或是人为干扰,a 到达 n' 的时间被延迟到了节点 m 之后。这里,“?”描述节点之间的偏序关系<sup>[1]</sup>, $n < m$  表示在时序上 n 是 m 的前驱。电子支付协议对消息到达的时间顺序较认证协议更为敏感,消息的延迟将可能影响交换的公平性。因此,我们定义延迟迹形式化地描述消息延迟现象。另外,消息发送迹( $\rightarrow$ )和节点转换迹( $\Rightarrow$ )的定义见文献[1]。

下面,我们给出 EMH 协议交换成功时,三种串空间状态描述。

第一种情况是不存在消息丢失,协议在交换阶段成功完成,则串空间状态如图 1。

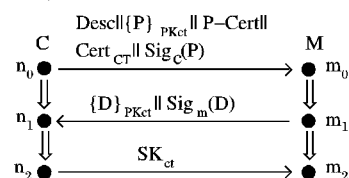


图 1 串空间状态 1

由图 1 可见,当交换结束时,C 获得正确的 D,同时 M 获得有效支付 P。D 是否符合 C 的要求通过 Desc 和 M 对 D 的签名保证,而 P 的有效性通过 CB 和 C 对 P 的签名以及 CB 对  $\{P\}_{PKct}$  签名保证。

第二种情况是消息 Mes. 5:  $SK_{ct}$  丢失,在等待一定时间后 M 发起争端解决,获得 TTP 的支持而最终交换成功。串空间状态如图 2 所示。

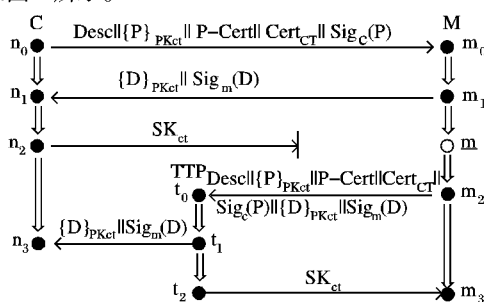


图 2 串空间状态 2

与状态 1 类似,通过 TTP 的支持,M 也能获得支付凭证 P 的解密密钥,从而获得 P。图中,节点 m 处的空心圆(O)表

示  $\text{term}(m) = \emptyset$ 。

第三种情况是消息  $\text{Mes. 4: } \{D\}_{PK_{ct}} \parallel \text{Sig}_m(D)$  丢失,在等待一定时间后  $M$  发起争端解决,获得 TTP 的支持而最终交换成功。串空间状态如图 3。

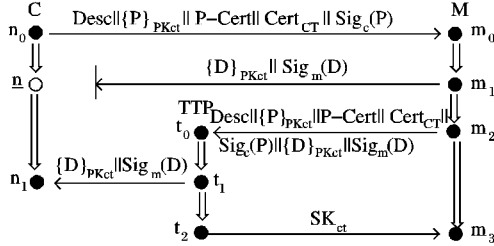


图3 串空间状态3

与状态2类似,通过 TTP 的支持,C 和 M 都能获得各自期望的信息。

**定理1** EMH 协议满足有效性。

**证明** 定理1的正确性是显然的,由上面的串空间状态图可以看出,如果 C 和 M 都是诚实的,能按照协议定义执行,且协议正确完成时,由于与 TTP 的通信信道是弹性信道,则 C 能获得期望的数字产品 D, M 也能获得有效支付凭证 P,即 EMH 协议能满足有效性定义。

### 3.3.2 EMH 协议碰撞性分析

根据碰撞性定义,我们假设 C 和 M 都可能是不诚实的,考虑 EMH 协议未正确执行时各情况。

第一种情况是 M 收到 Mes. 3 后,终止协议,这时串空间状态如图 4。

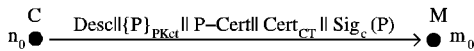


图4 串空间状态4

此时,EMH 协议串空间定义如下。

**定义7** EMH 串空间  $\square_1$  由三种类型的串组成:

- 1) 攻击者串  $s \in P$ , 这里,  $P$  的定义参见文献[1];
- 2) C 串  $s \in C[C, M, \text{Desc}, P, P\text{-Cert}, \text{Cert}_{CT}]$ , C 串由下面的串集合组成:

$$\langle + \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c} \rangle;$$

- 3) M 串  $s \in M[C, M, \text{Desc}, P\text{-Cert}, \text{Cert}_{CT}, *]$ , M 串由下面的串集合组成:

$$\langle - \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c} \rangle.$$

这里, \* 表示 P, 由于 M 并未获得解密密钥  $SK_{ct}$ , 因此 M 不能获得 P, 为了区分, 我们用 \* 表示。

**命题1** C 未能获得数字产品 D, 即在 EMH 串空间  $\square_1$  中不存在节点  $n$  使得含有 D 的项  $t \in \text{term}(n)$ 。

**证明** 首先, 我们考查 C 串和 M 串, 由定义 7, 显然不存在节点  $n$  使得消息  $t \in \text{term}(n)$ , 这里  $D \in t$ 。接着, 我们考查攻击者串, 由假设, 外部攻击者并不拥有数字产品, 即 D 不可能起源于外部攻击者, 则考查所有可能的攻击者串  $s \in P$ , 不存在节点  $n \in s$  使得包含 D 的消息  $t \in \text{term}(n)$ 。因此可得, 在 EMH 串空间  $\square_1$  中不存在节点  $n$  使得包含 D 的消息  $t \in \text{term}(n)$ , 即 C 未能获得数字产品 D。得证。

**命题2** M 未能获得支付凭证 P, 即在 EMH 串空间  $\square_1$  中, 不存在节点  $n$  使得  $P \in \text{term}(n)$ , 且不存在节点  $n'$  使得  $SK_{ct} \in \text{term}(n')$ 。

**证明** 首先考查 C 串和 M 串, 由定义 7, 不存在节点  $n$  和  $n'$  使得消息  $P \in \text{term}(n)$  且  $SK_{ct} \in \text{term}(n')$ 。接着考查攻击者串, 由假设, 外部攻击者并不拥有有效支付凭证 P 和密钥

$SK_{ct}$ , 即 P 和  $SK_{ct}$  不可能起源于外部攻击者。考查所有攻击者串  $s \in P$ , 则不存在节点  $n$  和  $n'$  使得消息  $P \in \text{term}(n)$  且  $SK_{ct} \in \text{term}(n')$ 。因此可得, 在 EMH 串空间  $\square_1$  中, 不存在节点  $n$  使得  $P \in \text{term}(n)$ , 且不存在节点  $n'$  使得  $SK_{ct} \in \text{term}(n')$ , 即 M 未能获得支付凭证 P。得证。

命题1和命题2表明在状态4, 协议满足碰撞性。

第二种情况是 C 收到 Mes. 4 后终止协议, 这时, C 已经获得 D, 而 M 可发起争端解决阶段, 通过 TTP 获得 P, 这种情形与前面的状态2和3类似。

第三种情况是 M 收到 Mes. 3 后, 直接发起争端解决阶段, 此时, 又存在两种情形: 一是 TTP 收到 Mes. 6 后, 验证不通过而否决 M, 则此种情形与第一种情况相同; 二是 TTP 收到 Mes. 6 后, 验证通过, 发送 Mes. 7 和 Mes. 8。由于假定与 TTP 的信道属于弹性信道, 则 Mes. 7 和 Mes. 8 总是能够到达 C 和 M, 串空间状态如图 5。

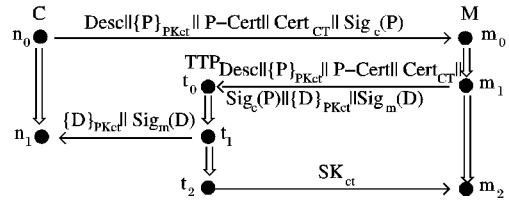


图5 串空间状态5

此时, EMH 协议串空间定义如下。

**定义8** EMH 串空间  $\square_2$  由四种类型的串组成:

- 1) 攻击者串  $s \in P$ , 这里,  $P$  的定义参见文献[1];
- 2) C 串  $s \in C[C, M, T, \text{Desc}, P, P\text{-Cert}, D, \text{Cert}_{CT}]$ , C 串由下面的串集合组成:

$$\langle + \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c}, \\ - \{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m} \rangle;$$

- 3) M 串  $s \in M[C, M, T, \text{Desc}, P, P\text{-Cert}, D, \text{Cert}_{CT}, SK_{ct}]$ , M 串由下面的串集合组成:

$$\langle - \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c}, \\ + \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c} \parallel \{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m}, - SK_{ct} \rangle;$$

- 4) T 串  $s \in T[C, M, T, \text{Desc}, P, P\text{-Cert}, D, \text{Cert}_{CT}, SK_{ct}]$ , T 串由下面串集合组成:

$$\langle - \text{Desc} \parallel \{P\}_{PK_{ct}} \parallel P\text{-Cert} \parallel \text{Cert}_{CT} \parallel \{h(P)\}_{PK_c} \parallel \{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m}, + \{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m}, + SK_{ct} \rangle.$$

状态5与状态2和3并不相同, 在状态2和3假定 C 和 M 是诚实的, 而在状态5则假设双方都可能是不诚实的, 那么我们需要考查 P 是否为有效支付凭证, 而且 D 是否符合 C 的描述。

**命题3** M 获得有效支付凭证 P, 即在 M 串中, 存在符号为“-”的节点  $n$  和  $n'$  使得  $\{P\}_{PK_{ct}} \in \text{term}(n)$  且  $SK_{ct} \in \text{term}(n')$ , 并且  $h(\{P\}_{PK_{ct}}) = \text{hep}$ 。

**证明** 由定义 8, M 串中存在符号为“-”的节点  $m_0$  和  $m_2$  使得  $\{P\}_{PK_{ct}} \in \text{term}(m_0)$  且  $SK_{ct} \in \text{term}(m_2)$ , 即 M 获得 P。同时, P 的有效性由 CB 确保,  $SK_{ct}$  的有效性由 TTP 确保, 则 M 获得有效支付凭证 P。得证。

**命题4** C 未获得符合描述的数字产品 D。

**证明** 由定义 8, C 串存在符号为“-”的节点  $n_1$  有  $\{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m} \in \text{term}(n_1)$ ,  $\{D\}_{PK_{ct}} \parallel \{h(D)\}_{PK_m}$  起源于图 5 中 M 串节点  $m_1$ , 我们考查子串序列  $m_1 \rightarrow t_0 \Rightarrow t_1 \rightarrow n_1$ , 在  $t_0$  节点, TTP 需要验证数字产品 D 是否符合描述 Desc, 在

EMH 串空间  $\square_2$  中 Desc 起源于 C 串节点  $n_0$ , 经由 M 串转发到  $t_0$  节点, 但是 C 并未对 Desc 进行签名以防止消息被篡改, 因此, Desc 存在被篡改的可能。假设 M 在转发的过程中对 Desc 进行篡改, 同时, 我们引入延迟迹, 延迟消息 Mes. 7 的到达时间, 此时串空间状态如图 6。

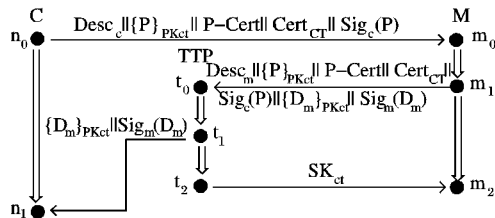


图 6 串空间状态 6

由图 6 可以看出, TTP 可验证  $D_m$  符合描述  $Desc_m$ , 而  $Desc_e \neq Desc_m$ 。因此, C 不能获得符合描述 ( $Desc_e$ ) 的数字产品 D。得证。

这里, 延迟迹  $t_1 \hookrightarrow n_1$ , 描述恶意实体延迟消息 Mes. 7 到达  $n_1$  节点的时间, 使得 M 相对于 C 较早获得 Mes. 8, 从而获得优势。

**定理 2** EMH 协议不满足碰撞性。

定理 2 可由命题 3 和命题 4 得出, 因为在状态 6 中, M 获得了有效支付凭证 P, 而 C 未能获得符合描述的数字产品 D, 不满足碰撞性定义。

**定理 3** EMH 协议不满足公平性。

定理 3 可由定理 1 和定理 2 直接推出。定理 1 表明 EMH 协议满足有效性, 即当交换双方都诚实的情况下, 协议能有效地进行 P 和 D 的交换。定理 2 表明 EMH 协议不满足碰撞性, 即存在一种情形使得 M 获得有效支付 P 而 C 未能获得有效的数字产品 D。

### 3.3.3 EMH 协议改进

由前面的分析可以看出, EMH 协议的缺陷在于缺乏对消息项 Desc 的数据一致性保护, 因此我们对消息 Mes. 3 作如下改进, 以防止恶意实体对 Desc 的篡改:

Mes. 3:  $Desc \parallel \{P\}_{PKct} \parallel P-Cert \parallel Cert_{CT} \parallel Sig_c(P \parallel Desc)$

则消息 Mes. 6 也相应的变为:

Mes. 6:  $Desc \parallel \{P\}_{PKct} \parallel P-Cert \parallel Cert_{CT} \parallel Sig_c(P \parallel Desc) \parallel \{D\}_{PKct} \parallel Sig_m(D)$

此时, TTP 可检验 C 对 P 和 Desc 的签名, 防止对 Desc 的篡改, 在上述状态 6 中, 有  $Desc_e = Desc_m$ , 那么 C 最终会得到符合描述的 D (虽然可能会有一定的延迟)。这时, 协议公平性也得到满足。

## 4 结语

本文采用扩展的串空间模型来分析电子支付协议的公平性。串空间模型使用节点因果关系的有向图来表示协议的运行轨迹, 能够直观地描述协议运行状态, 是一种有效的安全协议形式化分析方法。考虑到串空间理论原本用于分析传统的身份认证协议, 而电子支付协议与认证协议存在两个主要不同。一是协议目标不同, 认证协议主要分析认证性, 而支付协议主要关注公平性问题; 二是协议的攻击者模型不同, 认证协议主要考虑来自协议外部的攻击, 而支付协议则需要防范与之交易的对等实体的欺骗行为。基于此, 本文扩展了串空间理论, 增加了描述消息丢失和延迟的形式化方法。实例分析

表明, 扩展的串空间方法能有效分析电子支付协议的公平性。相对于同类型的其他方法<sup>[12-18]</sup>, 新方法具有直观性的优点, 能清晰地描述协议状态和实体行为。另外, 本文指出了 EMH 协议存在的安全缺陷, 并提出了改进意见。

### 参考文献:

- [1] THAYER F J, HERZOG J C, GUTTMAN J D. Strand spaces: Proving security protocols correct [J]. Journal of Computer Security, 1999, 7(2/3): 191-230.
- [2] FABREGA F, HERZOG J, GUTTMAN J. Honest ideals on strand space [C]// Proceedings of the IEEE Computer Security Foundations Workshop XI. California: IEEE Computer Society, 1998: 66-77.
- [3] ALARAJ A, MUNRO M. An efficient fair exchange protocol that enforces the merchant to be honest [C]// Proceedings of the Collaborative Computing: Networking, Applications and Worksharing. New York, USA: IEEE Computer Society, 2007: 196-202.
- [4] PAGNIA H, GARTNER F C, PAGNIA H, et al. On the impossibility of fair exchange without a trusted third party, TUD-BS-1999-02 [R]. Darmstadt, Germany: Darmstadt University of Technology, Department of Computer Science, 1999.
- [5] KREMER S. Formal analysis of optimistic fair exchange protocols [D]. Brussels, Belgium: University of Libre de Bruxelles, 2003.
- [6] KREMER S, MARKOWITZ O, ZHOU JIANYING. An intensive survey of non-repudiation protocols [J]. Computer Communications, 2002, 25(17): 1606-1621.
- [7] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchange [C]// 4th ACM Conference on Computer and Communications Security. New York: ACM, 1997: 8-17.
- [8] EVEN S, GOLDBREICH O, LEMPEL A. A randomizing protocol for signing contracts [J]. Communications of the ACM, 1985, 28(6): 637-647.
- [9] BENOR M, GOLDBREICH O, MICALI S, et al. A fair protocol for signing contracts [J]. IEEE Transactions on Information Theory, 1990, 36(1): 40-46.
- [10] ZHOU J, GOLLMANN D. A fair non-repudiation protocol [C]// Proceedings of 1996 IEEE Symposium on security and Privacy. Washington, DC: IEEE Computer Society, 1996: 55-61.
- [11] ASOKAN N. Fairness in Electronic Commerce [D]. Waterloo, Canada: University of Waterloo, 1998.
- [12] PAGNIA H, VOGT H, GARTNER F C. Fair exchange [J]. The Computer Journal, 2003, 46(1): 55-75.
- [13] QING SIHAN, LI GAICHENG. A formal model of fair exchange protocols [J]. Science in China Series F: Information Sciences, 2005, 48(4): 499-512.
- [14] KAILAR R. Accountability in electronic commerce protocols [J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313-328.
- [15] 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.
- [16] 陈庆锋, 白硕, 王驹, 等. 电子商务安全协议及其非单调动态逻辑验证 [J]. 软件学报, 2000, 11(2): 240-250.
- [17] 沈海峰, 薛锐, 黄河燕. 用串空间分析公平交换协议 [J]. 小型微型计算机系统, 2006, 27(1): 62-68.
- [18] 王涛, 郭荷清, 姚松涛. 串空间方法分析协议公平性的研究 [J]. 计算机工程与应用, 2004, 40(35): 17-21.
- [19] SYVERSON P, MEADOWS C. A logical language for specifying cryptographic protocol requirements [C]// Proceedings of the 1993 IEEE Symposium on Research on Security and Privacy. Washington, DC: IEEE Computer Society, 1993: 165-177.
- [20] SCHNEIDER S. Verifying authentication protocols with CSP [C]// Proceedings of the 10th IEEE Computer Security Foundations Workshop. Washington, DC: IEEE Computer Society, 1997: 3-17.
- [21] PAULSON L C. The inductive approach to verifying cryptographic protocols [J]. Journal of Computer Security, 1998, 6(1): 85-128.
- [22] DOLEV D, YAO A C. On the security of public key protocols [J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.