电子商务协议的串空间分析*)

刘义春[1] 张焕国[2]

(广东商学院广东省电子商务重点实验室 广州 510320)[1] (武汉大学计算机学院 武汉 430072)[2]

摘 要 电子商务协议常常具有复杂结构,协议可能由多个子协议组合而成。因此,电子商务协议的安全分析较认证协议更为复杂。传统的信念逻辑不适宜分析电子商务协议。Kailar 逻辑适宜分析电子商务协议的可追究性,但不适宜分析协议的公平性。本文介绍并扩展了串空间逻辑,分析了 ISI 支付协议的串,并证明其不满足公平性。还提出一种新的串节点路径法,用以分析了 ASW 协议,该协议系由多个子协议组成的分支结构协议,通过串空间分析证明了该协议的公平性。通过对两个协议的分析,分别提供了对电子商务在线交易协议和离线交易协议的形式化分析方法。

关键词 串空间,电子商务协议,公平性,串节点路径

Strand Spaces Analysis of Electronic Commerce Protocols

LIU Yi-Chun[1] ZHANG Huan-Guo[2]

(Guangdong Key Lab of Electronic Commerce, Guangdong University of Business Studies, Guangzhou 510320)[1]

(School of Computer Science and Technology, Wuhan University, Wuhan 430072)[2]

Abstract The electronic commerce protocols often have more complex structures than authentication protocols, and a protocol might be composite of multiple sub-protocols, so the security analysis of electronic commerce protocols is more complex than the analysis of authentication protocols. Traditional belief logic is not suitable for analyzing the electronic commerce protocol. Kailar logic is suitable for analyzing the accountability of commerce protocol and it is not suitable for fairness analysis. In this paper, the strand space model is described and expanded, and the ISI protocol is proven unfair by analyzing its strands. Based on strand space model, a universal strand node path method is presented to analyze the ASW protocol, which consists of multiple sub-protocols with branch structure, and the strand space analysis shows that the ASW protocol is fair. The formal analysis methods are proposed for electronic commerce exchange protocols with on-line TTP and off-line TTP by analyzing ISI protocol and ASW protocol.

Keywords Strand space, Electronic commerce protocol, Fairness, Strand node path

1 引言

随着电子商务应用的普及和发展,电子商务协议的研究越来越为人们所关注。在电子商务这一概念出现之前,信息安全领域的研究工作主要是围绕认证、存取控制、机密性和数据真实性、完整性而展开的。电子商务的出现则将公平性这一安全问题摆在了人们的面前。电子商务协议仅仅满足数据机密性、真实性和完整性还不够,一个安全的电子商务协议必须满足公平性。

电子商务协议公平性要求,在协议执行的任何阶段,参与协议的任何一方主体都不占优势[1]。公平性是电子商务协议最重要、最基本的性质。在现有电子商务研究中,对协议公平性大都进行手工分析,而缺少有效的形式化分析手段。

形式化分析方法以其严密的数学理论基础和广泛的适应性,代表了电子商务安全研究的发展方向。然而,目前安全协议的形式化分析研究多集中于对认证协议和密钥交换协议的分析,对电子商务协议的形式化分析则研究较少。

电子商务协议是一种特殊的安全协议,电子商务协议结构较认证协议和密钥交换协议远为复杂,协议执行不一定是顺序结构,有时含有条件分支或循环等非顺序执行。一个电子商务协议还可能是若干子协议的复合体。因此,电子商务协议的形式化分析迥异于认证协议和密钥交换协议,而有其自身特色,需要选择适宜的形式化方法,并对形式逻辑进行扩展,以有效地分析电子商务协议。

1983 年,Dolev 和 Yao 发表了安全协议发展史上的一篇重要的论文[2],将安全协议本身与安全协议所具体采用的密码系统分开,在假定密码系统是"完善"的基础上讨论协议本身的正确性、安全性。

Burrows 等提出的 BAN 逻辑[3]试图证明协议主体相信某个公式,主要适应于认证协议和密钥交换协议,目的是查找、分析安全协议中的漏洞,防止可能的假冒、篡改等协议攻击,不适宜分析电子商务交易协议的公平性。

Kailar 逻辑[4]通过对 BAN 逻辑进行改造,目的是协议主体能够向第三方证明另一方对某个公式负责,因此 Kailar 逻辑能用于证明电子商务协议的不可否认性。但是,作为一种基于推理的逻辑,Kailar 逻辑仍然不能分析协议的公平性,并缺乏对签名密文的分析机制[5]。

Ryan 提出使用 CSP 逻辑和模型检测工具 FDR 来分析协议[6]。基于进程代数的模型检测方法 CSP 试图检测或构造协议可能存在的攻击集合,建立一个运行协议的有限状态

*)国家自然科学基金项目(No60673071);浙江省自然科学基金项目(Y106802);浙江省教育厅科技计划项目(20060239)。刘义春 博士,副教授;张焕国 教授,博士生导师。

系统模型，然后使用状态检测工具 FDR 进行协议安全性分析。Lowe 使用 CSP 发现了 NSPK 协议存在的中间人攻击[7]。Heintze 等和 Schneider 等分别利用 CSP 逻辑成功地对 NetBill 系统和 DigiCash 系统进行原子性分析[8]。但使用 CSP 进行协议分析时，需要进行过多的非常抽象晦涩的进程描述和通信通道描述，且需要价格昂贵的专用协议分析工具，因此对研究工作带来一定的困难。

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[9,10]，分析了 Kailar 逻辑的缺陷[5]，对 Kailar 逻辑进行了改进，并提出了一种新的不可否认逻辑[11]，弥补了 Kailar 逻辑的一些缺陷。白硕等提出用非单调动态逻辑系统 NDL 分析电子商务交易协议[12,13]，并已对 SET 的一部分业务流程成功地进行了 NDL 验证。

Guttman 和 Thayer Fabrega 等结合了 NRL 协议分析器、CSP 模型检测技术以及 Paulson 的归纳证明的思想，基于消息代数理论提出新一代安全协议分析方法——串空间理论[14~16]。与 CSP 等协议分析方法相比，串空间模型更为简洁与直观，特别是通过有向图的辅助使得分析过程十分清晰。

由于串空间技术基于消息代数的特点并具有诸多优良性质，使得我们能尝试使用其进行电子商务协议的形式化分析。本文通过对串空间基本理论进行扩展，提出一种“串节点路径分析”方法，对两个著名的电子商务协议——ISI 协议[17]和 ASW 协议[18]进行公平性分析。

2 串空间理论

基于消息代数理论的串空间模型是一种结合定理证明和协议迹的混合分析方法。串空间理论使用“串”的概念描述协议的参与方发送消息和接收消息的行为，不同协议参与方的串组成串空间，表示协议的运行，串空间运行于代数结构上。消息代数定义了串空间的数据结构，以及数据项之间的关系。原始的串空间理论设计用于认证协议的形式化分析，描述对象和操作类型涉及面较窄。因此，需要根据具体分析目标进行适当的扩展。

2.1 消息代数

原始的消息代数中只包含了原子项、连接项和密文项的描述，我们需要在模型中加入对散列操作、签名操作以及加密解密等操作的描述，因此也相应地需要加入一些新的数据集合。

定义 1 设 A 表示协议的参与者交换的全部消息的集合，称为项空间，A 中的元素称为项，其元素是由下述集合生成：

- T：协议中的原子项；
- K：协议使用的密钥项。

其中 K，T 两两不相交。

在消息空间 A 上的操作包括：

- 加密运算 $encr: K\times A\to A$
- 解密运算 $decr: K\times A\to A$
- 连接运算 $join: A\times A\to A$
- Hash 运算 $hash: A\to A$
- 签名运算 $sign: K\times A\to A$
- 密钥映射 $key: A\to K$

$k\in K$ 的逆密钥表示为 k^{-1}。对于 $a,b,m\in A, k\in K$，我们将 $encr(k,m)$ 操作表示为 $\{m\}_k$，将 $decr(k,m)$ 操作表示为 $\{m\}_{k^{-1}}$，将 $join(a,b)$ 表示为 (a,b) 或者 ab，将 $hash(a)$ 表示为 $H(a)$，Hash 值的集合称为散列值空间 H；将 $sign(k,m)$ 表示为 $[m]_k$。

我们将形如 $\{m\}_k$、$H(m)$、$[m]_k$ 的项称为 A 上的操作项，将 T∪K 中的项称为原子项，原子项和操作项统称简单项，使用连接操作的项称为连接项。

定义 2 对于项 $h,g,g',g''\in A, k\in K$，h 称为 g 的子项，记为 $h\sqsubset g$，如果有下列之一：

(1) $h,g\in T\cup K$ 且 $h=g$；

(2) $g=(g',g'')$，且 $h\sqsubset g'$ 或 $h\sqsubset g''$ 或 $h=g$；

(3) $g=\{g'\}_k$，且 $h\sqsubset g'$ 或 $h=g'$。

其中，满足条件(1)、(2)的子项称为明文子项。

显然，子项关系 $\sqsubset$ 是一种传递、自反的关系。在这个项代数的结构上，协议参与者的行为表示发送或接收这些消息项的一个有限动作序列，即一个串 s 表示为：$(\langle\sigma_1,a_1\rangle,\cdots,\langle\sigma_n,a_n\rangle)$。其中 $\langle\sigma_n,a_n\rangle$ 称为一个有符号项，$\sigma_i\in\{+,-\}(1\leqslant i\leqslant n)$ 分别表示发送和接收，$a_i\in A\ (1\leqslant i\leqslant n)$，相应的 a_i 称为无符号项。$(\pm A)^*$ 表示有符号项的有限序列集，$(\langle\sigma_1,a_1\rangle,\cdots,\langle\sigma_n,a_n\rangle)\in(\pm A)^*$。协议参与方包括合法方和入侵者，相应的串也分为正常串和入侵串，这些串构成了串空间。

2.2 串空间和丛

定义 3 令 A 是给定的项空间，A 上的串空间定义为一个具有迹 tr 的集合 Σ，满足 $tr:\Sigma\to(\pm A)^*$。

定义 4 给定串空间 Σ，以及 $s\in\Sigma$，

(1) $\langle s,i\rangle$ 是串上的节点，其中 i 表示节点 $\langle s,i\rangle$ 在 s 中的序号 $(1\leqslant i\leqslant height(tr(s)))$，$height(tr(s))$ 表示串 s 的迹长度)。所有节点的集合表示为 N。

(2) 对于 $n\in N$，$term(n)=(tr(s))_i$ 表示串 s 上的第 i 个有符号项，$uns\_term(n)=((tr(s))_i)_2$ 表示串 s 上的第 i 个无符号项。

(3) 对于 $n_1,n_2\in N$，存在边 $n_1\to n_2$，当且仅当 $term(n_1)=+a$，且 $term(n_2)=-a$，其中 $a\in A$，表示 n_1 先于 n_2 发生，且 n_1 发送的消息被 n_2 接收到。

(4) 对于 $n_1,n_2\in N$，如果 $n_1=(s,i)$，$n_2=(s,i+1)$，则存在边 $n_1\Rightarrow n_2$，表示在串 s 上，节点 n_1 发生后，n_2 马上发生了。

(5) 项 t 出现于节点 n，当且仅当 $t\sqsubset term(n)$。

(6) 假设 I 是一个无符号项集合，节点 n 是 I 的入口点，当且仅当 $term(n)=+t(t\in I)$。

(7) 无符号项 t 源于节点 n，当且仅当 n 是集合 $I=\{t':t\sqsubset t'\}$ 的入口点。无符号项 t 是唯一源于项，当且仅当 t 源于唯一的节点 n。

定义 4 中定义了节点集合和节点上存在的两个边关系，这样串空间的基本结构可以表示为一个直连图 $(N,(\to\cup\Rightarrow))$。在这个图结构上，就可以形式化描述协议运行的情况。

定义 5 已知节点集合 N 及其上的边构成的图 $(N,(\to\cup\Rightarrow))$，假设有 $N_B\subset N$，$\to_B\subset\to$，$\Rightarrow_B\subset\Rightarrow$，且 $B=(N_B,(\to_B\cup\Rightarrow_B))$ 是 $(N,(\to\cup\Rightarrow))$ 的子图，如果 B 满足：

(1) B 是有限的；

(2) 如果 $n_2\in N_B$，且 $term(n_2)$ 的符号是负的，则存在唯一的节点 n_1 满足 $n_1\to_B n_2$；

(3) 如果 $n_2\in N_B$，且 $n_1\Rightarrow_B n_2$，则有 $n_1\in N_B$；

(4) B 不是有环的；

则称 B 是一个丛(Bundle)。

如果 n 属于丛 B 的节点集合，则称节点 n 在丛上，简记为 $n\in B$；如果串 s 上的节点都在 B 的节点集上，则称串 s 在丛 B

上，简记为 $s\in B$。丛是多个节点通过边关系→和⇒连接而成的单向图。串 s 在丛 B 中的高度即是满足 $\langle s,i\rangle\in B$ 的最大的 i，表示为 $B\text{-}height(s)$。串 s 在 B 上的迹表示为 $B\text{-}trace(s)=\langle(tr(s))_1,\cdots,(tr(s))_m\rangle$，其中 $m=B\text{-}height(s)$

串空间理论中有如下两个重要的假设，称为自由假设：

公理 1 对于 $t_1,t_2\in A$，且 $k_1,k_2\in K$，有

$\{t_1\}_{k_1}=\{t_2\}_{k_2}\Rightarrow t_1=t_2,k_1=k_2$

公理 2 对于 $t_1,t_2,t_3,t_4\in A$ 且 $k\in K$，有

(1) $(t_1,t_2)=(t_3,t_4)\Rightarrow t_1=t_3,t_2=t_4$

(2) $(t_1,t_2)\neq\{t_3\}_k$

(3) $(t_1,t_2)\notin T\cup K$

(4) $\{t_1\}_k\notin T\cup K$

为了对电子商务协议进行有效分析，我们通过增加下面的自由假设对串空间逻辑进行扩展：

公理 3 对于 $t\in A$ 且 $k\in K$，有

$\{\{t\}_k\}_k^{-1}=t$

新增的公理 3 使得串空间逻辑能用于分析含有加密消息项的电子商务协议。

这三个公理描述了信息空间 A 是由集合 T 和 K 通过操作 *encr*、*decr* 和 *join* 自由生成的代数。

2.3 电子商务协议的公平性

本节所述电子商务协议中，规范定义了三种角色：买方 C、卖方 M、可信机构 T。它们对应的协议串为买方串、卖方串和可信方串。

电子商务支付协议的公平性可分为强公平性和弱公平性两类，强公平性的实现不需借助外部争议解决子协议，弱公平性的实现需要借助外部争议解决子协议。可用串空间逻辑术语如下描述：

定义 6(强公平性) 某一支付协议的串空间为 Σ，该协议被称为强公平的，若下面条件满足：

i)如果买方串中有项节点含有表示有效支付的子项且该项节点符号为正，那么买方串中一定存在项节点含有表示商品的明文子项且该项节点符号为负；

ii)如果卖方串中有一个项节点，其消息项含有表示商品的明文子项，且该项节点符号为正，那么卖方串中一定存在另外项节点含有表示支付的子项且该项节点符号为负。

定义 7(弱公平性) 某一支付协议的串空间为 Σ，该协议称为弱公平的，若下面条件满足：

i)如果买方串中有项节点含有表示有效支付的子项且该项节点符号为正，那么买方串中存在含有表示商品的明文子项或能获得买方已进行有效支付的仲裁证据子项的项节点且该项节点符号为负；

ii)如果买方串中存在含有表示商品的明文子项的项节点，且该项节点符号为负，那么卖方串中一定存在含有表示支付子项或表示已向买方成功交付商品的仲裁证据子项的项节点且该项节点符号为负。

3 ISI 支付协议分析

3.1 ISI 支付协议

南加州大学的 ISI 支付协议[17]用于提供一个在安全的网络上进行的实时电子支付协议。协议描述如下：

1) $A\rightarrow B:+K_{ab}$

2) $B\rightarrow A:\{K_b\}_{K_{ab}}$

3) $A\rightarrow B:\{\{coins\}_{K_{cs}^{-1}},SK_a,K\_ses,s\_id\}_{K_b}$

4) $B\rightarrow CS:\{\{coins\}_{K_{cs}^{-1}},SK_b,transaction\}_{K_{CS}}$

5) $CS\rightarrow B:\{\{new\_coins\}_{K_{cs}^{-1}}\}_{SK_b}$

6) $B\rightarrow A:\{\{amount,Tid,date\}_{K_b^{-1}}\}_{SK_b}$

ISI 支付协议是公平的仅当如下条件成立：B 能得到有效的支付且 A 能得到支付收据；或当 B 不能得到有效支付时 A 亦不能得到支付收据。

3.2 ISI 协议的串空间分析

ISI 支付协议的协议丛如图 1 所示。

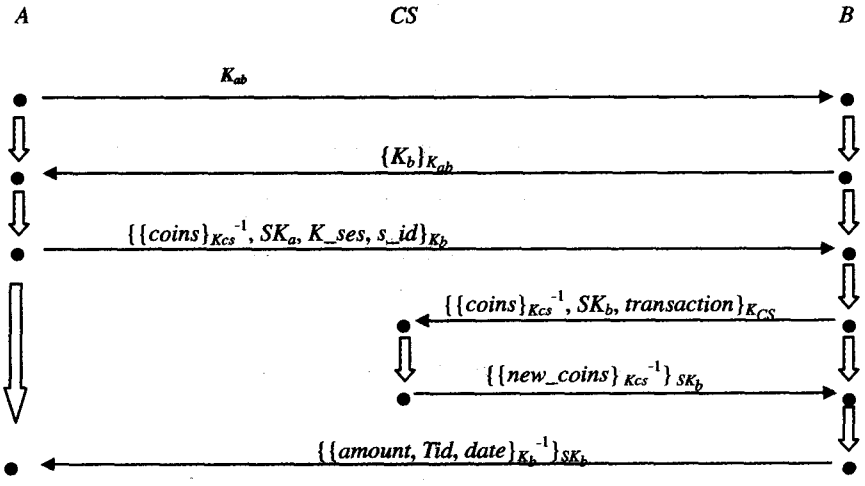

图 1 ISI 支付协议

A、B 诚实地执行协议时协议将执行完毕，当一方行为异常或出现通信故障时协议将被中止。协议正常完成时，协议的串节点集为最大；协议中途停止的情况下，协议串节点集是正常完成协议串节点集的子集。支付者 A 的协议串的串节点如下：

$\langle s_1,1\rangle$ $+K_{ab}$

$\langle s_1,2\rangle$ $-\{K_b\}_{K_{ab}}$

$\langle s_1,3\rangle$ $+\{\{coins\}_{K_{cs}^{-1}},SK_a,K\_ses,s\_id\}_{K_b}$

$\langle s_1,4\rangle$ $-\{\{amount,Tid,date\}_{K_b^{-1}}\}_{SK_b}$

可能的协议发起者串 s_1 有如下 4 种情形：

1) $\langle+K_{ab},-\{K_b\}_{K_{ab}},+\{\{coins\}_{K_{cs}^{-1}},SK_a,K\_ses,s\_id\}_{K_b},-\{\{amount,Tid,date\}_{K_b^{-1}}\}_{SK_b}\rangle$

2)〈$+K_{ab}$，$-\{K_b\}_{K_{ab}}$，$+\{\{coins\}_{K_{cs}^{-1}}$，$SK_a$，$K\_ses$，$s\_id\}_{K_b}$〉

3)〈$+K_{ab}$，$-\{K_b\}_{K_{ab}}$〉

4)〈$+K_{ab}$〉

在情形 2)下，串节点〈s_1，3〉含有一个代表有效支付的子项，但该串中没有任何串节点含表示收据的子项。亦即 A 发送了有效的支付但得不到有效的支付收据。由此判定，ISI 协议不满足公平性。

4 ASW 协议分析

4.1 ASW 协议

Asokan 提出了著名的通用交易协议—ASW 协议[18]。一个两方 ASW 协议在参与方 O、R 之间交换商品，T 为可信方。有关信息项介绍如下：

- $item_X$　某方 X 将提供的数字商品项。
- $descr_X$　X 提供的商品的描述。
- fit($descr$，$item$)　评价商品项是否符合商品描述。
- commit($item$)　对数据项 $item$ 的提交，用作发送方不可否认证据。
- open($item$，key，com)　评估数据项与其提交项是否相符。

ASW 协议由三个子协议组成：交易子协议、O 发起的争议解决子协议、R 发起的争议解决子协议。图 2 描述了交易子协议，图 3 和图 4 分别描述 O 和 R 发起的争议解决子协议。

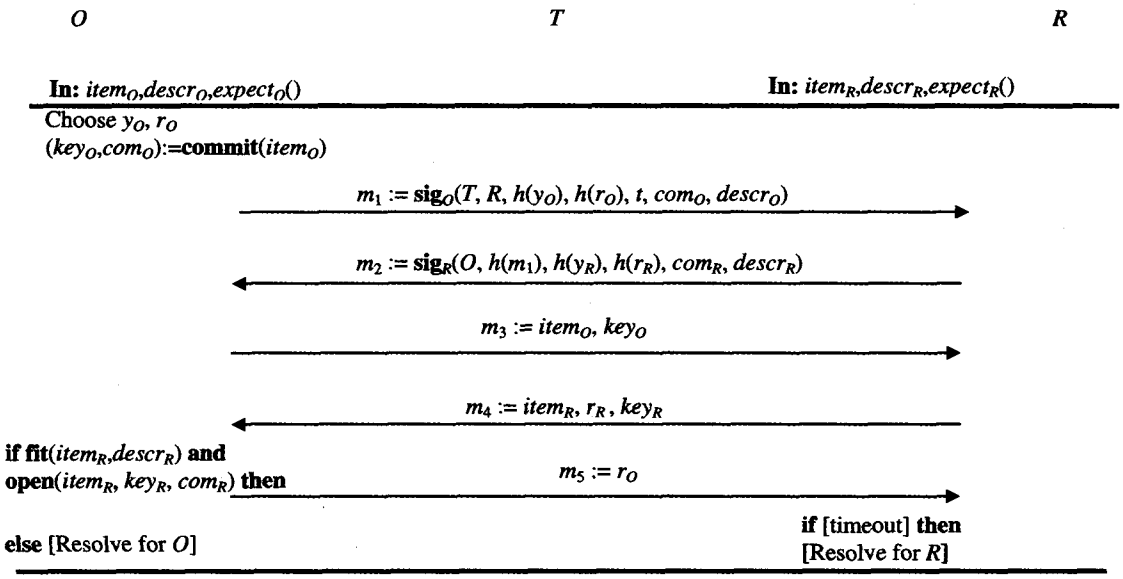

图 2　ASW 协议的交易子协议

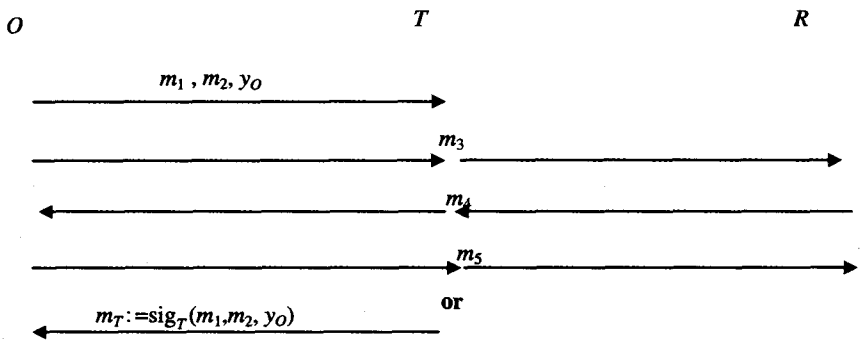

图 3　ASW 协议的发起方解决子协议

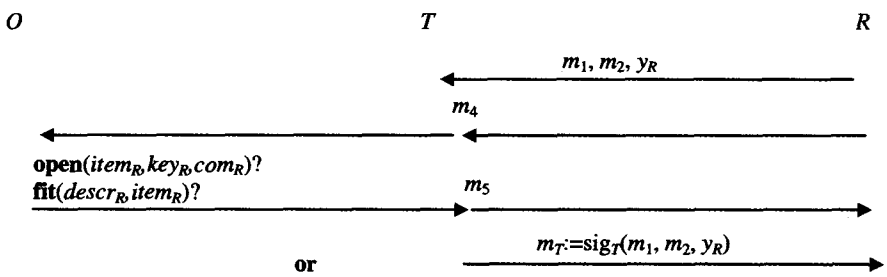

图 4　ASW 协议的应答方解决子协议

4.2 ASW 协议的串空间分析

表 1 ASW 协议 O 和 R 的串节点

node	message item	node	message item
$\langle s_1,1\rangle$	$+m_1$	$\langle s_2,1\rangle$	$-m_1$
$\langle s_1,2\rangle$	$-m_2$	$\langle s_2,2\rangle$	$+m_2$
$\langle s_1,3\rangle$	$+(item_O, key_O)$	$\langle s_2,3\rangle$	$-(item_O, key_O)$
$\langle s_1,4\rangle$	$-(item_R, r_R, key_R)$	$\langle s_2,4\rangle$	$+(item_R, r_R, key_R)$
$\langle s_1,5\rangle$	$+r_O$	$\langle s_2,5\rangle$	$-r_O$
$\langle s_1',1\rangle$	$+(m_1, m_2, y_O)$	$\langle s_2',1\rangle$	$-(item_O, key_O)$
$\langle s_1',2\rangle$	$+(item_O, key_O)$	$\langle s_2',2\rangle$	$+(item_R, r_R, key_R)$
$\langle s_1',3\rangle$	$-(item_R, r_R, key_R)$	$\langle s_2',3\rangle$	$-r_O$
$\langle s_1',4\rangle$	$+r_O$	$\langle s_2'',1\rangle$	$+(m_1, m_2, y_R)$
$\langle s_1',5\rangle$	$-sig_T(m_1, m_2, y_O)$	$\langle s_2'',2\rangle$	$+(item_R, r_R, key_R)$
$\langle s_1'',1\rangle$	$-(item_R, r_R, key_R)$	$\langle s_2'',3\rangle$	$-r_O$
$\langle s_1'',2\rangle$	$+r_O$	$\langle s_2'',4\rangle$	$-sig_T(m_1, m_2, y_R)$

ASW 协议由多个带 if-then 分支结构的字协议组成。在此提出一种新的串节点路径分析法分析协议的公平性。

设 s_1、s_2 分别是交易子协议中 O、R 的串，s_1'、s_2' 分别是发起方解决子协议中 O、R 的串，s_1''、s_2'' 分别是应答方解决子协议中 O、R 的串。ASW 协议串节点如表 1 所示。

诚实的发起方串节点路径如图 5 所示，诚实的应答方串节点路径如图 6 所示，协议发起方 O 和应答方 R 均有多条串路径。

当协议发起方 O 诚实地执行协议时，其可能的串节点路径如下：

Path 1: $\langle(s_1,1)\rangle$

Path 2: $\langle(s_1,1),(s_1,2)\rangle$

Path 3: $\langle(s_1,1),(s_1,2),(s_1,3),(s_1,4),(s_1,5)\rangle$

Path 4: $\langle(s_1,1),(s_1,2),(s_1,3),(s_1',1),(s_1',2),(s_1',3),(s_1',4)\rangle$

Path 5: $\langle(s_1,1),(s_1,2),(s_1,3),(s_1',1),(s_1',2),(s_1',5)\rangle$

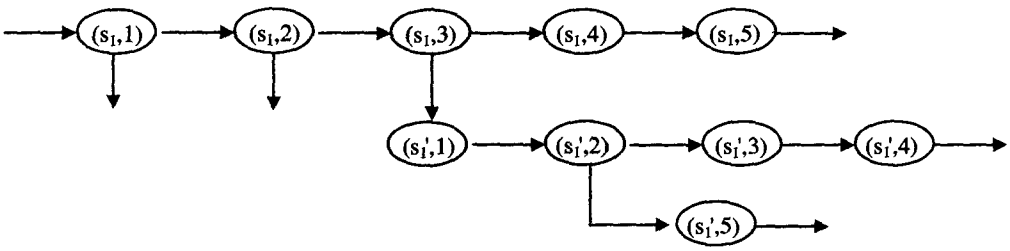

图 5 诚实的发起方串节点路径

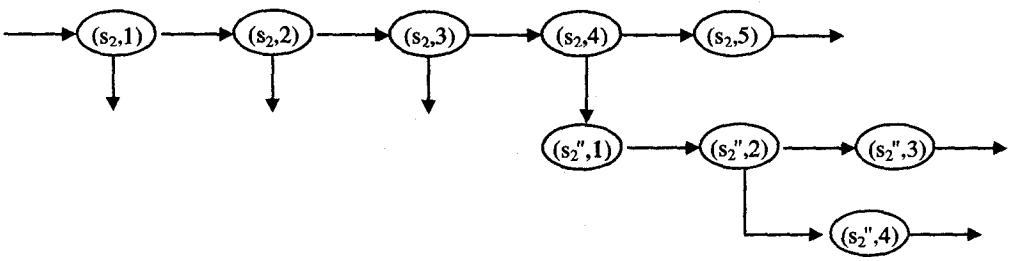

图 6 诚实的应答方串节点路径

在路径 1 和路径 2，无任何节点含子项 $item_O$，亦即 O 没有发送任何商品。

在路径 3，节点 $(s_1,3)$ 包含项 $(item_O, key_O)$，节点 $(s_1,5)$ 含有项 r_O，且二节点符号皆为“+”；而节点 $(s_1,4)$ 包含项 $(item_R, r_R, key_R)$ 且符号为“−”。

在路径 4，节点 $(s_1,3)$ 含子项 $(item_O, key_O)$，节点 $(s_1', 4)$ 含有项 r_O，且符号皆为“+”；而节点 $(s_1',3)$ 含有项 $(item_R, r_R, key_R)$ 且符号为“−”。

在路径 5，节点 $(s_1,3)$ 含子项 $(item_O, key_O)$，且符号为“+”；而节点 $(s_1',5)$ 含有用作发起方已发送商品的证词的项 $sig_T(m_1, m_2, y_O)$ 且符号为“−”。

以上分析表明，如果发起方 O 已将商品项 $(item_O, key_O)$ 发送给应答方 R，O 能收到来自 R 的商品项 $(item_R, r_R, key_R)$ 或来自可信方的已发送商品证词项 $sig_T(m_1, m_2, y_O)$。

当应答方 R 诚实地执行协议时，其可能的串节点路径如下：

Path 1: $\langle(s_2,1)\rangle$

Path 2: $\langle(s_2,1),(s_2,2)\rangle$

Path 3: $\langle(s_2,1),(s_2,2),(s_2,3)\rangle$

Path 4: $\langle(s_2,1),(s_2,2),(s_2,3),(s_2,4),(s_2,5)\rangle$

Path 5: $\langle(s_2,1),(s_2,2),(s_2,3),(s_2,4),(s_2'',1),(s_2'',2),(s_2'',3)\rangle$

Path 6: $\langle(s_2,1),(s_2,2),(s_2,3),(s_2,4),(s_2'',1),(s_2'',2),(s_2'',4)\rangle$

在路径 1、路径 2 和路径 3，无任何节点含子项 $item_R$，亦即 R 没有发送任何商品。

在路径 4，节点 $(s_2, 4)$ 包含项 $(item_R, r_R, key_R)$ 且符号为“+”；而节点 $(s_2,3)$ 包含项 $(item_O, key_O)$，节点 $(s_2,5)$ 包含项 o，且二节点符号皆为“−”。

在路径 5，节点 $(s_2,4)$ 包含项 $(item_R, r_R, key_R)$ 且符号为“+”；而节点 $(s_2, 3)$ 包含项 $(item_O, key_O)$，节点 $(s_2'', 3)$ 包含项 o，且二节点符号皆为“−”。

在路径 6，节点 $(s_2,4)$ 包含项 $(item_R, r_R, key_R)$ 且符号为“+”；而节点 $(s_2, 3)$ 包含项 $(item_O, key_O)$ 和用作应答方证词的项 “$sig_T(m_1, m_2, y_R)$”，且节点符号皆为“−”。

上述分析表明，如果协议应答方 R 已经将商品项($item_R$，r_R，key_R)发送给发起方 O，R 能获得来自 O 的 ($item_O$，key_O，r_O)或证词项 $sig_T(m_1, m_2, y_R)$。

对双方串节点路径的分析表明，当一方已发送商品给另一方后，必能获得其所期望的商品项或来自可信方的证词，没有任何一方较另一方处于优势，即 ASW 协议是弱公平的。

结束语 现有的形式化分析研究多集中在认证协议和密钥交换协议。而电子商务协议具有更为复杂的协议结构，如分支结构，或由多个子协议组成，使得难以使用传统的信念逻辑进行分析。本文对串空间逻辑进行了扩展，使之能分析带密文项的电子商务协议。还提出串节点路径分析法，以利用串空间逻辑分析带复杂结构的协议，从而给出了一种较为通用的电子商务协议形式化分析方法。文中成功地对 ISI 支付协议和 ASW 协议进行串空间分析，形式化地证明了 ISI 协议不满足公平性，而 ASW 协议则满足公平性。基于串空间逻辑的复杂协议自动分析器是我们今后研究的方向。

参 考 文 献

1 Asokan N. Fairness in electronic commerce:[PhD thesis]. University of Waterloo, 1998
2 Dolev A, Yao A C. On the security of public-key protocols. IEEE Transactions on Information Theory, 1983, 2(29): 198～208
3 Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1):18～36
4 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996, 22(5): 313～328
5 周典萃，卿斯汉，周展飞. Kailar 逻辑的缺陷. 软件学报，1999，10(12):1238～1245
6 Ryan P, Schneider S. Modelling and analysis of security protocols. Addison-Wesley Publishing Co, 2000
7 Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. Software Concepts and Tools, 1996, 17: 93～102
8 Heintze N, Tygar J D, Wing J, et al. Model checking electronic commerce protocols. In: Proc. 2nd USENIX Workshop on Electronic Commerce, 1996. 147～164
9 卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2000. 127～147
10 卿斯汉. 一种新型的非否认协议. 软件学报，2000，11(10)：1338～1343
11 周典萃，卿斯汉，周展飞. 一种分析电子商务协议的新工具. 软件学报，2001，12(9)：1318～1328
12 白硕，隋立颖，陈庆锋，等. 安全协议的验证逻辑. 软件学报，2000，11(2)：213～221
13 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. 软件学报，2000，11(2)：240～250
14 Thayer F J, Herzog J C, Guttman J. Strand spaces: Why is a security protocol correct? In: Proc the 1998 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1998. 160～171
15 Thayer F J, Herzog J C, Guttman J. Honest ideals on strand space. In: Proc. 11th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1998
16 Thayer F J, Herzog J C, Guttman J. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(2-3): 191～230
17 Medvinsky G, Neuman B C. Netcash: a design of practical electronic currency on the Internet. In: Proc. ACM Conf. on Computer and Communication Security. New York: ACM Press, 1993. 76～82
18 Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. In: Proc. 4th ACM Conf. on Computer and Communication Security. ACM Press, 1997. 6～17

(上接第 80 页)

提出的方案计算开销就比较高。反之，如果大量的邻居节点认证只是为了获得网络的使用权限，那么我们的方案就可以取得比较好的效果。

结论 本文在分析以往移动自组网密钥协商协议的基础上，综合移动自组网的实际需要，提出了一种适用于移动自组网的密钥协商方案，减轻了节点的计算和通信开销，同时实现了身份认证的功能。本文所提出的方案比较简单，安全性较好，计算和通信开销小，因此非常适合于移动自组网这种能量和计算资源有限的网络。我们下一步的研究目标是结合匿名认证方案和 MPLS 标签交换的局部性来实现移动自组网的匿名安全路由，并结合信任相关的理论来阻挡来自网络的内部的攻击，实现节点回收的功能。

参 考 文 献

1 Zhu S, Xu S, Setia S, et al. Establishing Pair-wise Keys for SecureCommunication in Ad Hoc Networks: A Probabilistic Approach. In: IEEE ICNP, 2003
2 Kong J, Zerfos P, Luo H, et al. Providing Robust and UbiquitousSecurity Support for MANET. In: IEEE ICNP, 2001
3 Narasimha M, Tsudik G, Yi J H. On the Utility of Distributed Cryptography in P2P and MANETs: The Case of Membership Control. In: IEEE ICNP, 2003
4 Jarecki S, Saxena N, Yi J H. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In: ACM SASN, 2004
5 Joux A. A one-round protocol for tripartite Diffie-Hellman. In Algorithmic Number Theory Symposium -ANTS-IV, Springer-Verlag LNCS1838, 2000. 385～394
6 Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the Eurocrypt 2003. LNCS 2656, Warsaw: Springer-Verlag, 2003. 416～432
7 Smart N P. An identity-based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002, 38: 630～632
8 Chen L, Kudla C. Identity based authenticated key agreement protocols from pairings. CSFW'03, 2003. 219～236
9 Ertaul L, Lu W M. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). In: Boutaba R, Almeroth K, Puigjaner R, et al. eds. Networking 2005. LCNS 3462, Canada: University of Waterloo, Springer-Verlag GmbH, 2005. 102～113
10 Zhang Y, Liu W, Lou W W. Anonymous Communications in Mobile Ad Hoc Networks. IEEE INFOCOM, 2005

(上接第 86 页)

息，可大大减轻可信第三方的负担。

结束语 本文采用基于身份的密码体制作为基础，提出了一套切实可行、安全高效的邮件安全认证方案，该方案系统开销小，安全级别较高，有效地实现了 Web 方式电子邮件系统中的安全认证问题。系统实际运行结果表明，该认证系统结果正确，运行速度较快，运行状况良好。

参 考 文 献

1 Shamir A. Identity-based cryptosystems and signature schemes [J]. In: Advances in Cryptology-CRYPTO84, Vol. 196 of LNCS, Springer-Verlag, 1984. 47～53
2 Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing [C]. Advance in Cryptology-CRYPTO 2001. LNCS 2139, 2001. 213～229
3 Boneh D, Franklin M. Short Signatures from Weil Pairing [C]. Boyd C ASIACRYPT 2001. Berlin: Springer-Verlag, 2001. 514～532
4 Menezes A, Okamoto T, Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field [J]. IEEE Trans on Information Theory, 1993, 39(5): 1639～1646
5 Hess F. Efficient identity based signature schemes based on pairings [C]. In SAC'02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography. Springer-Verlag, 2003. 310～324
6 Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography [M]. Publishing House of Electronics Industry, 2005, 8: 5～20