# 统一的安全属性形式化描述方法的研究*)

谢鸿波[1,2] 吴远成[1] 周明天[1]

(电子科技大学计算机科学与工程学院 成都 610054)[1] (重庆通信学院三系数据链教研室 重庆 400035)[2]

**摘 要** 安全属性的基于特定分析方法和限于特定属性的形式化描述严重影响了安全协议形式化分析方法的有效性和适用性。为解决这个问题,本文提出了一种统一的形式化描述方法,即通过属性动作之间的匹配关系来表达协议的安全属性。用这种方法详细分析了认证属性、保密属性以及公平性属性的形式化表达。通过比较分析,该方法与其他方法相比,具有准确、简洁和扩展性强的特点,在总体上优于其他方法。

**关键词** 协议分析,形式化分析方法,安全属性

## On Unifying the Formal Method to Depict the Security Properties

XIE Hong-bo[1,2] WU Yuan-chen[1] ZHOU Ming-tian[1]

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[1]

(Data Like Staff Room of the 3rd Department, Chongqing Communication College, Chongqing 400035, China)[2]

**Abstract** The formal expression of security properties based on special analysis methods and used to special properties has largely affected the validity and applicability of the formal security protocol analysis. In order to solve this problem, a unifying method based on trace is been formally presented. In this method, the security properties are expressed as the match relations between property actions. This method can be used to express most kinds of security properties. As an example, it has been used to analyse the formal express of the authentication, secret, and fairness properties. Compared with other methods, this method is simpler, more expressive and has great expansibility.

**Keywords** Protocol analysis, Security properties, Formal analysis

## 1 引言

安全属性的形式化描述是安全协议形式化分析方法中的一个关键问题。近些年来,许多形式化分析方法[1-4]被用来对安全协议进行安全性分析。这些方法用自己的形式化语言来描述安全属性,并证明之。类 BAN 逻辑[1]对安全属性的描述是用类似"$A|\equiv B|\equiv(A \xleftarrow{K} B)$"这样的谓词逻辑来表示的。串空间方法[2]通过节点与丛的关系来表示协议的认证属性和保密属性。基于 CSP 的方法[3]使用"信号-事件"机制来描述认证和保密属性。SPI 方法[4]通过"进程等价"概念来描述安全属性。这些方法针对特定属性的形式化描述比较复杂,并且难以扩展到其他安全属性,从而影响了这些方法的有效性和适用范围。

在分析了大量的安全协议及其分析方法之后,本文提出了一种统一的安全属性形式化描述方法,即通过属性事件之间的匹配关系来表达协议的安全属性。利用该方法本文详细分析了认证、保密和公平性属性的形式化表达。该方法简单直观,具有很强的扩展性。本文的主要贡献在于,通过统一的安全属性形式化描述方法,可以准确地描述安全属性,并进一步扩展协议的形式化分析方法的适用范围。

本文第 2 节简单介绍 SPI 演算与迹方法相结合的形式化安全协议分析方法。第 3 节阐述安全属性统一的形式化描述方法,以及该方法对认证、保密和公平性属性的分析。第 4 节比较分析了该方法与现有安全协议分析方法中安全属性描述的比较。最后总结本文工作及贡献,提出未来的工作。

## 2 基于 SPI 演算的迹方法简介

本文采用 SPI 演算[4]作为协议的描述语言。为了更准确地描述变量在进程中的限制范围,本文对 SPI 演算中的算法结构做了必要的修改。其语法如下:

| | | |
|---|---|---|
| $L,M,N::=$ | | 术语 |
| | $n$ | 名字 |
| | $(M,N)$ | 对 |
| | $0$ | 零 |
| | $x$ | 变量 |
| | $\{X\}_N$ | 加密 |
| $P,Q,R::=$ | | 进程 |
| | $\underline{0}$ | 零 |
| | $\overline{M}\langle N\rangle.P$ | 输出 |
| | $M(x).P$ | 输入 |
| | $P\|Q$ | 组合 |
| | $(\nu n).P$ | 限制 |
| | $!P$ | 重复 |
| | $[M \text{ is } N].P$ | 匹配 |
| | $\text{De } x \text{ as } \{M\}_d.P$ | 解密 |
| | $\text{En } \{M\}_d \text{ as } x.P$ | 加密 |

与 SPI 演算不同的是"加密"和"解密"结构。这两个结构明确地将密文数据与变量绑定在一起,准确地说明了变量 $x$ 在后续进程 $P$ 中的限制范围。

SPI 演算能准确地表示协议运行的并发会话,这对于描述协议真实的运行环境是非常重要的。表 1 通过大嘴蛙协议

*)基金项目:国家 863 项目 863-104-03-01 课题资助。谢鸿波 博士研究生,主要研究领域为网络与信息系统安全、分布对象技术;吴远成 博士研究生,主要研究领域为网络与信息系统安全、分布对象技术;周明天 教授,博士生导师,主要研究领域为计算机网络、分布对象技术、并行分布处理和网络与信息系统安全。

的例子说明了这一点。

表 1 大嘴蛙协议的 SPI 演算表示

| | |
|---|---|
| 1. A→S: {K}Kas | A= En {K}Kas as x. $\overline{C}$ ⟨x⟩. En {d}K as y. $\overline{C}$ ⟨y⟩. A′ |
| 2. S→B: {K}Kbs | S=C (x). De x as { x′}Kas. En { x′}Kbs as y. $\overline{C}$ ⟨y⟩. 0 |
| 3. A→B: {d}K | B= C(x). De x as {x′}Kbs. C (y). De y as { y′}x′. B′ |
| WMF=! A|! S|! B | |

SPI 演算的操作语义采用文献[5]的迹的术语来表示。迹是一个动作序列，该序列来自进程与环境的交互。迹的结构如下所示：

| | |
|---|---|
| $\sigma::=$ | 迹 |
| $0$ | 空迹 |
| $a::\sigma$ | 动作序列 |
| $a::=$ | 动作 |
| $\mathrm{New}(I,V)$ | 产生临时值或密钥 |
| $I\triangleright\overline{M}\langle N\rangle$ | 输出 |
| $I\triangleright M(x)$ | 输入 |
| $\mathrm{Run}(I_1,I_2)$ | 初始认证 |
| $\mathrm{Commit}(I_1,I_2)$ | 完成认证 |

**定义 2.1**(符号迹和配置) 一个符号迹是一个动作串 $\sigma\in \mathrm{Act}^*$，且(a) $\mathrm{en}(\sigma)=0$，(b) 每个 $\sigma_1,\sigma_2,a,x$，如果 $\sigma=\sigma_1.a.\sigma_2$，且 $x\in V(a)-V(\sigma_1)$，那么 $a$ 一定是输入动作。一个符号配置 $\langle\sigma,P\rangle_s$，是由符号迹和一个进程组成，且 $\mathrm{en}(P)=0$，$V(P)\subseteq V(\sigma)$。

其中，$\mathrm{Act}^*$ 表示由动作组成的动作串集合，$\mathrm{en}(P)$ 表示 $P$ 中的环境变量集合，$V(P)$ 表示 $P$ 中的变量集合。

**定义 2.2**(解决形式) 如果每个 $\sigma_1,\sigma_2,a\langle M\rangle$，$\sigma=\sigma_1.a\langle M\rangle.\sigma_2$，都有 $\sigma_1\rightarrow M$，那么我们说，迹 $\sigma$ 是一个解决形式($sf$)。其中，符号"$\sigma\rightarrow M$"表示迹 $\sigma$ 可以得到消息 $M$。

$SF(\sigma)$ 是迹 $\sigma$ 经过提炼规则(见文献[5]定义 5.6)可以得到的满足解决形式 $sf$ 的迹的集合。

**定理 2.3** 设 $\sigma$ 为一个符号迹，属性 $Pr=\alpha\rightarrow\beta$，且 $V(\alpha)\subseteq V(\beta)$，$V(\alpha)\cap V(\beta)=0$。当且仅当以下条件为真：每个 $\theta$，有 $\alpha\in_\theta \mathrm{act}(\sigma)$，且每个 $\sigma'\in \mathrm{SF}(\sigma\theta)$，$\sigma'=\sigma\theta\theta'$，有 $\alpha\theta\,\theta'$ 发生在 $\beta\theta\,\theta'$ 之前成立，那么 $\sigma\vdash \mathrm{Pr}$。其中，符号"$\alpha\rightarrow\beta$"表示动作 $\alpha$ 发生在动作 $\beta$ 之前，$\mathrm{act}(\sigma)$ 是迹 $\sigma$ 中的动作集合。

在文献[5]中，认证协议的安全性分析变成了定理 2.3 的认证属性满足证明。该定理的证明，以及更多的定义、定理及其证明详见文献[5]。

## 3 安全属性的形式化描述

### 3.1 统一的形式化方法

安全协议通过协议运行时的消息交换来实现协议目标。协议消息由协议数据、密钥、临时值、实体名等子数据通过组合、加密/解密、签名/验证等方法计算得到。协议消息有两层含义：一个是原始含义，即消息包含了哪些数据；一个是外延含义，即消息发送的目的。协议目标被攻破往往是因为消息外延含义被滥用导致的。

单个消息的外延含义并不足以表示协议的安全属性。协议运行是有序动作组成的，因此，协议的安全属性必定包含在这些有序的协议动作及其相应的消息外延含义中。于是，在迹方法[5]的基础上，我们提出了统一的安全属性形式化描述方法。

属性动作用来表示与属性有关的协议消息的外延含义。当协议参与者发送或接收一个与协议安全属性相关的消息时，产生一个相应的属性动作来描述该属性消息的外延含义。由于迹是一个有序动作串，迹的动作之间存在着某种时序和数量上的匹配关系，因此，安全属性完全可以用属性动作之间的某种匹配关系来表示。

我们用 $A_{Pr}$ 表示协议的属性动作集合，即：$A_{Pr}=\{a_1,a_2,\cdots,a_n\}$。属性动作之间的匹配关系表明了一个属性动作到另一个属性动作的映射，我们用 $R$ 表示这种映射的集合，即：$A_{Pr}\times A_{Pr}\in R, R=\{r_1,r_2,\cdots,r_m\}$。其中，$r_i$ 是一个二元关系，$a_1\ r_i\ a_2$，表示动作 $a_1$ 和 $a_2$ 满足匹配关系 $r_i$。因此，协议的安全属性就可以表示成有序对 $(a_i,a_j)$ 的集合，即：$Pr=\{(a_i,a_j)\mid a_i,a_j\in A_{Pr}, a_i\times a_j\in r, r\in R\}$。根据迹方法[5]，协议运行时的属性动作可以表示成 $a\theta$，其中 $\theta$ 是一个替换函数，将协议运行消息映射到属性动作中变量。那么，协议运行时的安全属性就可以表示成 $(a_1\theta,a_2\theta)$，即：如果属性动作 $a_1,a_2$ 满足关系 $r$，那么运行时的属性动作 $a_1\theta,a_2\theta$ 也必须满足关系 $r$，否则协议的安全属性不能被满足。

在统一的安全属性形式化描述方法下，安全属性的满足性判定定理为 3.1。

**定理 3.1** 设 $\sigma$ 为一个符号迹，属性 $(\alpha,\beta)$，其匹配关系为 $r$，且 $V(\alpha)\subseteq V(\beta)$，$V(\alpha)\cap V(\beta)=0$。当且仅当以下条件为真：

每个 $\theta$，有 $\alpha\in_\theta \mathrm{act}(\sigma)$，且每个 $\sigma'\in \mathrm{SF}(\sigma_\theta)$，$\sigma'=\sigma\theta\theta'$，有 $\alpha\theta\theta'$ 和 $\beta\theta\theta'$ 满足匹配关系 $r$，那么 $\sigma\vdash(\alpha,\beta)$。

### 3.2 认证属性的形式化描述

在大多数的形式化分析方法[2-6]中，对于认证属性的非形式化描述是这样的：在协议 P 中，如果当 $B$ 想与 $A$ 交谈时，他确实在与 $A$ 交谈，则表示向 $B$ 认证 $A$。这是实体认证，即：协议参与者向对方认证自己的身份。此外，还有消息认证[4,9,10]。消息认证的非形式化描述为：当消息 $M$ 被申明是由协议参与者 $A$ 产生时，则该消息确实是由 $A$ 在当前协议运行中产生的。

消息认证有两层含义，一个是消息确实是由合法参与者产生的，一个是消息确实是在当前协议运行中产生的。前者是通过消息的签名/验证来保证的。后者是通过属性动作的匹配关系来保证的，即发送认证消息，插入属性动作 $\mathrm{Run}_M(A,B,M)$，表示 $A$ 发起消息 $M$ 的认证过程，当接收者 $B$ 处理该消息时，插入属性动作 $Commit_M(B,A,M)$，表示 $B$ 确认消息 $M$。这两个属性动作存在这样的关系：认证发起动作与认证确认动作是一一对应的。即：每一个 $Commit_M$ 动作必然有一个相应的 $Run_M$ 动作发生在它之前。

除了用 $Run_I(A,B)$ 和 $Commit_I(B,A)$ 来表示属性动作外，实体认证的匹配关系与消息认证相似。

因此，认证属性可以表示成属性动作 $Run_X$ 和 $Commit_X$(其中 $X(\{M,I\})$，满足关系 $R_{Auth}=Run_X\ni Commit_X$，符号 $\ni$ 表示动作之间是一个单射关系，即：$Run_X$ 总是发生在 $Commit_X$ 之前，并且，如果属性动作 $Commit_X$ 发生 $n$ 次，那么与其相应的属性动作 $Run_X$ 至少发生 $n$ 次。

根据定理 3.1，协议认证属性的满足条件是：设 $\sigma$ 为协议的符号迹，如果 $\sigma\vdash Run_X\ R_{Auth}\ Commit_X$，那么我们说协议满足认证属性。

### 3.3 保密属性的形式化描述

保密属性的前提是：协议使用的密码算法是完善的[8]。也就是说，入侵者攻破保密属性是由协议运行的逻辑错误造

成的。在不同的协议中，对保密属性的要求是不一样的。有些协议的保密属性要求协议数据的保密，即在一个有人侵者的环境里，如果协议从不发布数据 $D$ 或任何可以用来计算 $D$ 的数据，那么协议保持数据 $D$ 的保密性[3,4,6]。而有些协议则要求数据与某个实体的关联性是保密的，即协议参与实体的身份与它产生的数据之间的关联保密，入侵者不知道某个数据 $D$ 是由谁产生的[7]。

根据本文的方法，当协议实体发送一个数据需要保密的消息 M 时，插入保密属性动作 $Secret(M)$，表示消息 $M$ 里的某些数据或信息（如上面说的消息数据之间的关联信息）需要保密。当接收者处理该消息时，插入保密属性动作 $Leak(M)$，表示消息 $M$ 中数据或者关联信息的泄漏。这两个属性动作的匹配关系是：泄漏动作产生的信息不是保密动作产生的信息，即：$R_{sc}=(\mathrm{Info}(Secret)\cap\mathrm{Info}(Leak)=0)$。其中，$\mathrm{Info}(a)$ 表示动作 $a$ 产生的信息。

根据定理 3.1，协议保密属性的满足条件是：设 $\sigma$ 为协议的符号迹，如果 $\sigma\vdash Secret\ R_{sc}\ Leak$，那么我们说协议满足保密属性。

### 3.4 公平属性的形式化描述

协议的公平性属性是没有被很好理解的，与认证属性、保密属性等相比，它更难于表达和验证。卿斯汉[12]认为公平性应该满足以下两个条件：1）正确执行协议后，应当保证发送方收到 EOR（Evidence Of Receipt），且接收方收到 EOO（Evidence Of Origin）；2）如果协议异常终止，协议应当保证通信双方都处于同等地位，任何一方都不占有任何优势，或者说，协议的执行在任何一步异常终止时，消息接收方收到 EOO，当且仅当消息发送方收到 EOR。S. Kremer[11]等人认为公平性涉及到不可否认协议、公平交换协议、合同签名协议以及基于证书的电子邮件协议等不同类型的协议。因此，对公平性的非形式化表述为：协议实体以一种没有人被愚弄的方式来交换他们的有效信息。

影响公平性的因素有两个：一个是信道是否可靠，即由于信道的原因使得参与者没收到相应的有效信息，从而造成实事上的不公平；另一个是参与者是否公平地执行协议，即参与者利用协议规范逻辑上的缺陷，使得自己在有效信息的占有上处于优势地位。因此，公平性属性应该包含两层含义：

1）实体在没有收到所希望的有效信息前，它不会发送自己的有效信息。

2）协议运行的任何阶段，协议通信双方处于同等地位，即：双方都不能获得比对方更多的有效信息。

有效信息具有类型和值两个属性，我们用符号 $m=\langle type,value\rangle$ 表示一个有效消息。

我们用属性动作 $Recv(i,j,M)$ 表示实体 $i$ 在步骤 $j$ 收到有效消息 $M$，用属性动作 $Send(i,j,N)$ 表示实体 $i$ 在步骤 $j$ 发送有效消息 $N$。根据第一层含义，这两个动作的匹配关系是：收到动作发生再发送动作之前，即：$R=Recv\Rightarrow Send$。根据定理 3.1，设 $\sigma$ 为协议的符号迹，如果 $\sigma\vdash\{Recv(i,j,M)\Rightarrow Send(i,k,N)$，$i$ 是协议发起者和响应者，且 $j\leqslant k$，其中 $M$ 是实体 $i$ 发送有效信息 $N$ 所希望得到的有效消息$\}$，那么满足公平属性的第一层含义。

我们用属性动作 $Own(i,j)$ 表示实体 $i$ 在协议运行步骤 $j$ 拥有的有效消息。第二层含义的匹配关系为：实体 $A$ 和 $B$ 在时刻 $j$ 具有的有效消息的类型是一一对应的，即：如果 $A$ 有一个有效消息的类型是临时值，那么 $B$ 一定有一个同样类型的有效消息。用符号 $Type(m)$ 表示有效消息 $m$ 的类型属性，那么该匹配关系可以表示成：$R=\{Own(A,j)\ni Own(B,j)\mid\forall m\in Own(A,j),\exists n\in Own(B,j),\text{and } Type(m)=Type(n),\text{and }\forall h\in Own(B,j),\exists k\in Own(A,j),\text{and } Type(h)=Type(k)\}$。根据定理 3.1，设 $\sigma$ 为协议的符号迹，如果 $\sigma\vdash Own(A,j)\ni Own(B,j)$，那么满足公平属性的第二层含义。

当安全协议满足 $\sigma\vdash\{Own(A,j)\ni Own(B,j)\text{ and }Recv(i,j,M)\Rightarrow Send(i,k,N)\}$ 时，我们称该协议满足强公平性，否则，满足第一层含义，我们称为时序公平性，满足第二层含义，我们称为消息公平性。

## 4 比较与分析

本节，我们将从准确性、简洁性、可扩展性和适用性四个方面来比较本文的方法与其他形式化分析方法中安全属性的表达方式。

类 BAN 逻辑用谓词“相信”构成的逻辑公式来表示协议目标。它的表达非常简洁，但准确性不足，如：在密钥建立协议中，协议目标表示为：$A\mid\equiv(A\overset{K}{\leftrightarrow}B)$。该协议目标应该包含两个含义，一个是 $A$ 确认与它通信的就是 $B$，即：实体认证，一个是密钥 $K$ 是 $A$ 和 $B$ 才知道的“好密钥”，即：消息保密。这个公式并没有很好地表达这两个含义。类 BAN 逻辑主要是关于认证的，它不能用逻辑公式来描述其他安全属性，如：保密属性、公平属性、匿名属性等，从而使它能分析的协议类型非常有限。

CSP 方法通过“信号-事件”机制来描述安全属性。与类 BAN 逻辑相比，它对安全属性的描述虽然要复杂一些，但要准确得多。如：在 CSP 方法中，保密属性表示为：signal. Claim_Secret. $a.b.m$ in $tr\Rightarrow\neg$leak. $m$ in $tr$）。但它不能表示除保密和认证属性之外的安全属性，因此，该方法能分析的协议类型有限。

串空间方法[2]通过节点与丛的关系来描述协议安全属性。在分析协议时，形式化的定理或命题被用来准确地描述它们之间的不同关系，以分别表示协议的认证和保密属性。显然，这种方式虽然能够比较准确地描述安全属性，但其表达方式比 CSP 方法更复杂一些。在扩展性方面，它与 CSP 方法一样局限在认证和保密属性上。

SPI 演算[4]通过“进程等价”概念描述安全属性。其描述方法比较简洁，如：认证属性表示为：$Inst(M)\cong(Instspec(M)$ for any $M$。“进程等价”比较准确地描述了协议规范描述的安全属性。基于 SPI 演算的迹方法[5]用动作时序上的先后关系来表示认证和保密属性，即：$\alpha\lrcorner\beta$，动作 $\alpha$ 发生在动作 $\beta$ 之前。这两种方法只能分析认证属性和保密属性，因此，适用范围是有限的。

本文的方法通过属性动作及其相互关系来表达安全属性，即：$\alpha R\beta$，动作 $\alpha$ 和 $\beta$ 满足匹配关系 $R$。属性表达式比较简洁。属性动作及其关系的定义，能够准确地描述安全属性的细节，如，类 BAN 逻辑中的 $A\models(A\overset{K}{\leftrightarrow}B)$ 可以被准确地描述为 $Run_I(B,A)\ni Commit_I(A,B)\text{ and }k\in\mathrm{Info}(Secret)\text{ and }k\notin$

（下转第 186 页）

表2 特征抽取对文本分类算法性能的影响情况

| 测试值 / 文档集编号 | MP | | MR | | MF1 | |
|---|---|---|---|---|---|---|
| | 特征抽取前 | 特征抽取后 | 特征抽取前 | 特征抽取后 | 特征抽取前 | 特征抽取后 |
| 1 | 0.64 | 0.74 | 0.63 | 0.73 | 0.63 | 0.73 |
| 2 | 0.67 | 0.77 | 0.61 | 0.72 | 0.64 | 0.74 |
| 3 | 0.65 | 0.71 | 0.66 | 0.75 | 0.65 | 0.73 |
| 4 | 0.68 | 0.76 | 0.65 | 0.73 | 0.66 | 0.74 |
| 5 | 0.65 | 0.72 | 0.61 | 0.77 | 0.63 | 0.74 |

从表2可以看出，经过特征抽取后，文本分类的MP，MR和MF1值被普遍提高了将近8个百分点，说明对特征词的抽取能为分类文本带来较高的精确度，在文本分类中应该引起足够重视。

**结束语** 本文提出一种基于混合并行遗传聚类的文本特征抽取方法，通过特征词的粗聚类、特征词的精聚类和特征重构，有效地消除了文本中的同义词和近义词现象以及强关联语义信息，降低了文本特征维数，为文本分类精度和效率的提高提供了有效的帮助。实验证明，该方法是一种有效的文本特征抽取方法。

本文主要研究了针对文本分类问题的特征抽取方法，但是对于通过特征词聚类挖掘出来的特征词之间的语义关联没有加以分析。下一步的工作将对特征词聚类挖掘出的语义关系进行分析，并以可视化方式描述特征词间的语义关联。

## 参考文献


[1] Mühlenbein H. Evolution in time and space-the parallel Genetic Algorithm [M]. Rawlins, Foundations of Genetic Algorithms. Morgan Kaufmann, 1991

[2] Liu Juan, Iba H. Selecting informative genes with parallel GA in tissue classification[J]. Genome Informatics, 2001, 3(12): 14-23

[3] Pettey C B, et al. A Parallel Genetic Algorithm// Proc. of the Second ICGA. 1987: 155-161

[4] Tanese R. Parallel genetic algorithm for a hypercube// Proc. of the second ICGA. 1987: 177-183

[5] Glover F. Future Paths for Integer Programming and Links to Artificial Intelligence [J]. Computers and Operations Research, 1986, 13: 533-549

[6] Glover F, Kelley J, Laguna M. Genetic algorithms and tabu search: a hybrids for optimization[J]. Computers Operations Research, 1995, 22(1): 111-134

[7] Lee L J. Similarity-based approaches to natural language processing. Ph. D. Thesis. Harvard University, 1997


(上接第174页)

Info( *Leak*)。在统一的描述方法下，通过扩定义新的属性及其关系，可以描述多种安全属性，如：公平属性。因此，本方法具有很强的扩展性和广泛的适用性。总体上来说，本方法优于其他方法，如表2所示。

表2 各种方法比较

| 方法 | 准确性 | 简洁性 | 可扩展行 | 适用性 |
|---|---|---|---|---|
| 属性统一描述方法 | 高 | 较高 | 高 | 高 |
| 类BAN逻辑 | 差 | 高 | 差 | 差 |
| CSP方法 | 高 | 中 | 中 | 中 |
| 串空间 | 高 | 差 | 差 | 中 |
| SPI演算 | 较高 | 高 | 中 | 中 |

**结束语** 安全属性的形式化描述是证明协议安全性的关键问题之一。不同的形式化分析方法对于安全属性有不同的形式化描述方法。然而，它们局限于具体的分析方法和少数的安全属性，不具备普遍性，从而影响了分析方法的使用范围和有效性。本文在迹方法的基础上，提出了一种统一的安全属性形式化描述方法。将安全属性抽象成属性动作及其匹配关系，在协议分析时，通过确定具体的属性动作和匹配关系，可以准确且一致地形式化描述协议的某个安全属性，使得基于迹的分析方法可以有更广泛的适用范围，分析更多类型的安全协议。本文还在这个方法下，具体分析了安全协议的认证、保密和公平性属性的形式化表达。通过比较分析，该方法与其他方法相比，具有准确、简洁和扩展性强的特点，在总体上优于其他方法。

## 参考文献


[1] Burrows M, Abadi M, Needham R. A logic of authentication. Technical Report 39, Digital Systems Research Center, 1989

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

[3] Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. Software-Concepts and Tools, 1996, 17: 93-102

[4] Abadi M, Gordon A D. A calculus for cryptographic protocols: The spi calculus. Information and Computation, 1999, 148(1): 1-70

[5] Boreale M. Symbolic trace analysis of cryptographic protocols// Proceedings of ICAL P01. volume 2076. LNCS 2076. Springer Verlag, 2001: 667-281

[6] Abadi M, Blanchet B. Analyzing security protocols with secrecy types and logic programs. Journal of the ACM, 2005, 52(1): 102-146

[7] Kremer S, Ryan M D. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus// Proceedings of the European Symposium on Programming (ESOP'05), Lecture Notes in Computer Science Series. Springer Verlag, 2005

[8] Dolev, Yao D. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2): 198-208

[9] Focardi R, Gorrieri R. A Classification of Security Properties. Journal of Computer Security, 1995, 3(1): 5-33

[10] Abadi M. Security protocols and their properties. In Foundations of Secure Computation, volume 175 of NATO Science Series: Computer & Systems Sciences. IOS Press, 2000: 39-60

[11] Kremer S, Markowitch O, Zhou J. An intensive survey of fair non-repudiation protocols. Computer Communications, 2002, 25(17): 1606-1621

[12] 卿斯汉. 电子商务协议中的可信第三方角色[J]. 软件学报, 2003, 14(11), 1936-1943