基于加密电路构造的移动代理保护安全模型的研究

郑 彦[1], 王汝传[1,2], 穆 鸿[1], 王海艳[1]
(1. 南京邮电大学计算机学院, 江苏南京 210003;
2 南京大学计算机软件新技术国家重点实验室, 江苏南京 210093)

摘 要: 本文主要讨论保护移动代理免受恶意主机攻击的问题. 在指出现有的基于"加密函数"的移动代理保护方法不足的同时作者提出了一种基于可信任元素的安全代理保护模型. 这种可信任元素不同于可信任硬件如智能卡和协处理器, 它是一种基于加密电路构造的第三方服务称为可信任服务. 文中给出了移动代理计算的形式化描述, 并说明了纯软件保护方法是不可行的, 在介绍完加密电路构造方法后给出了基本模型来说明如何借助于可信任服务实现安全性, 并对模型进一步扩充, 最后给出应用该模型的一个实例分析.

关键词: 移动代理; 加密电路构造; 安全性
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2006) 08-1410-05

The Research of Encrypted Circuit Construction Based Secure Model for Mobile Agent

ZHENG Yan[1], WANG Ru-Chuan[1,2], MU Hong[1], WANG Hai-Yan[1]
(1 College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China;
2 State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu 210093, China)

Abstract As a new technology, mobile agent shows a wide application in the field of network technology. However, security has been one of the crucial problems in the employment of mobile agents. In order to protect mobile agent against malicious hosts, some approaches have been proposed in the literature. A new protection model based on a trusted element is presented in this paper. The trusted element, which differs from traditional trusted hardware such as smart card or co-processor, offers a third party service based on an encrypted circuit construction. Procedure of constructing encrypted circuit is introduced and the way to use the trusted service to protect mobile agent is also described. An application example is given to show how to use the new model at the end of the paper.

Key words mobile agent; encrypted circuit construction; security

1 引言

移动代理技术是随着 Internet的发展而出现的一种新兴技术, 它较好的适应了 Internet的特点, 有效简化分布式系统的设计、实现和维护. 一般来讲, 移动代理是指一段独立的计算机程序, 它按照一定的规程, 能够自主的在异构的网络上移动, 代表用户完成特定的任务. 移动代理的优势主要有两点: 一方面, 它实现了计算向所需资源的靠拢, 这可以节省网络的带宽并具有异步功能; 另一方面, 允许程序动态发布到主机.

由于移动代理的诸多优点, 它在电子商务、移动计算、Internet信息的智能发现等方面都有较好的应用前景, 对移动代理技术的研究正成为学术界和工业界的热点之一. 移动代理的关键技术包括移动机制、通讯机制以及安全机制. 安全性是制约移动代理技术广泛使用的重要因素之一, 因此研究移动代理的安全问题具有重要意义.

移动代理的安全问题[1,2]主要包括三个方面: (1)保护移动代理通讯通道, (2)执行环境的保护, (3)移动代理的保护. 目前对前两个方面的研究已有不少成果, 例如沙箱模型、签名加密、检验传输代码等方法. 然而对移动代理的保护的研究还处于初步阶段, 因为移动代理是由主机执行的, 它不得不在主机环境中公开数据和代码, 也就冒着被

收稿日期: 2004-02-09; 修回日期: 2006-03-18
基金项目: 国家自然科学基金 (No. 60573141, No. 70271050); 江苏省自然科学基金 (No. BK2005146); 江苏省高技术研究计划 (No. BG2005037, No. BG2005038, No. BG2006001); 国家 863高技术研究发展计划 (No. 2005AA775050); 南京市高技术项目 (2006软资 105); 江苏省计算机信息处理技术重点实验室基金 (No. kjs050001, No. kjs06); 江苏省高校自然科学研究计划 (No. 05KJB520092)

恶意主机篡改、扫描甚至是终止的危险了, 这些显然给问题的解决带来了一定的难度. 有学者[3]提出可以借助密码学原理的协议来使得可以以一种安全的形式执行移动代理从而达到保护移动代理的目的. 然而, 大多数基于安全计算的协议需要经过多轮交互, 这在实际应用中是不可行的. 我们引入加密电路构造协议, 期望可以通过第三方元素的介入来达到减少交互次数和保护代理的目的. 引入第三方元素的方法一个很典型的例子是引入可信任硬件[4,5]. 主要方法是把移动代码下载到防篡改的硬件执行, 在代理离开时再对其进行加密. 但有一个前提就是假定所有的用户都信任硬件的制造商, 而且另外一点执行主机必须引入一个相对昂贵的硬件设备. 与之相对, 我们引入第三方元素称为可信任服务, 它有如下几个优点: (1)公共的, 费用可由多个代理应用共享, (2)独立的, 不依赖于特定应用可由一个独立实体维护, (3)基于软件的, 所需代价较小.

2　移动代理计算模型

在这一部分我们形式化描述移动代理计算并给出了我们给定的安全条件. 形式化模型被用来证明在没有其他措施的情形下, 完全由软件保护活动的移动代理是不可能的.

2.1　模型

一个基本的移动代理计算模型如图 1所示:

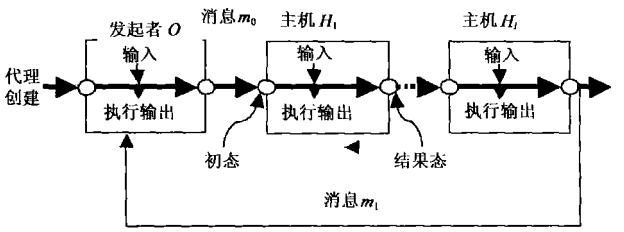

图 1　移动代理计算模型

它包括如下要素:

参与者: 一个发起者 O 和 l 个移动代理运行所在的主机 $H_1, H_2, \cdots, H_l$.

非交互式通讯: 每个参与者只发送和接收一个单独的消息. 我们用 m_0 来表示 O 发送给 H_1 的消息, m_j 表示 H_j 发送给 H_{j+1} 的消息, 其中 $j = 1, \cdots, l-1$, m_l 表示最后一个主机 H_l 返回给 O 的消息.

计算: 设移动代理的状态为集合 X 的一个元素. 它的初始态 x_0 由 O 决定. 设 H_j 的输入为集合 Y 的一个元素而 H_j 的输出为集合 Z 的一个元素 (输入和输出定义域对所有主机而言都是相同的). 在主机 H_j 上的计算用两个函数表示:

$$g_j: X \times Y \rightarrow X \text{ 和 } h_j: X \times Y \rightarrow Z$$

求出代理的新状态 $x_j = g_j(x_{j-1}, y_j)$ 和输出 $z_j = h_j(x_{j-1}, y_j)$, O 得到代理的最终态 $\xi = x_l \in X$. 函数 g_i 和 h_i 对所有的参与者都是已知的.

一个非交互的安全代理计算模型包含 $2l+2$ 个算法即 $A_0, A_1, \cdots, A_l, B_1, B_2, \cdots, B_l$ 及 D 从而对所有的 $j = 1, \cdots, l$ 和 $x_0 \in X, y_j \in Y$ 及相应的计算:

$$m_0 = A_0(x_0)$$
$$m_j = A_j(m_{j-1}, y_j), \text{其中 } j = 1, \cdots, l$$
$$z_j = B_j(m_{j-1}, y_j), \text{其中 } j = 1, \cdots, l$$
$$\xi = D(m_l)$$

满足下面两个条件

条件: $\xi = g_l(x_l, y_l)$ 并且 $z_j = h_j(x_{j-1}, y_j)$, 其中 $j = 1, \cdots, l$
$x_{j'} = g_{j'}(\cdots(g_2(g_1(x_0, y_1), y_2)\cdots), y_{j'})$, 其中 $j' = 1, \cdots, l-1$

保密性: 所有主机的输入、输出和计算对其他主机和发起者都是隐藏的(除了那些从输出得到的结果): O 只知道 ξ, 对 y_j 却是一无所知(除了来自 x_0 和 ξ 的结果), 类似的, H_j 只知道 z_j, 对 x_0 和 $y_{j'}$ $(j' < j)$ 一无所知(除了来自 z_j 和 y_j 的结果).

为简单起见, 模型假定代理访问所有主机的顺序是固定的. 它可以扩展以允许由 z_j 来决定访问次序. 方法是引入一个函数 $\pi: Z \rightarrow \{1, \cdots, l\}$, 而移动代理由 H_j 发送到 $H_{\pi(z_j)}$. 在只有一个主机 H 的移动代理应用中, 函数 g 得到 O 的输出 ξ 而 h 得到 H 的输出 z.

2.2　纯软件的保护方法

有学者[6,7]首先意识到纯软件的方法保护移动代理免受恶意主机的攻击对小程序而言使用加密技术还是切实可行的. 他们提出使用称为同态公钥加密方案的方法通过只处理密码来允许两个加密明文消息非交互的加或乘. 通过这种方法, 主机可以由一个多项式描述的隐藏的输入 x 计算任意的函数 g(·, y), 但这是在只有一个主机情形下.

这种方法后来被改进到有隐藏输入 x (可由对数级电路描述)的所有函数 g(·, y)的非交互计算. 随后又被进一步推广到任意函数, 规定他们可以用多项式尺度的电路描述. 他们还描述了如何用这种方法实现有多个主机的安全的移动代理应用.

然而, 所有的方案只是定位在为更新代理的状态和得到最后的结果的 g_j 的安全计算上, 但是忽略了如何实现 h_j 以便在主机 H_j 上得到输出. 更准确的说, 他们受到函数 h_j: $Y \rightarrow Z$ 的约束从而主机的输出不能依赖任何东西除了它自己的输入.

事实上, 不难看出这是在给定情形下能得到的最佳结果. 从另一方面看, 假定存在一个活动代理, 它输出一些值给它的主机. 例如, 在一个购物代理应用中声明是否接受商品. 为简单起见又假定, 代理的决定只取决于 H_j 给出的价格 y_j, 那它就会购买最便宜的商品. 代理的状态 $x_{j-1} = c$ 声明一个由发起者选择的安全阈值 c, 价格在这个下面, 它就会接受商品. 由于我们模型中的通讯约束, 它需在 m_{j-1} 和 y_j 上运行算法 B_j 产生 z_j, 然后 H_j 可以求出代理是否愿意购买 y_j 和 y_j 是否小于 c, 但是这不能阻止一个恶意主机再次用另一个 y_j 运行算法 B_j 并持续下去直到 c 值溢出.

这表明移动购物代理应用的纯软件保护方法是不可行的. 事实上, 我们可以得到下面的结论: 非交互的安全计算方案不存在, 特别的, 任何方案只要其中一些主机要知道的信息取决于代理的当前状态那它就是不安全的. 因此我们必须扩展上面的模型来获得活动的移动代理的保密性和完整性. 允许每个主机和发起者进行通讯可以解决先前提及的问题. 但这就破坏了移动代理这种模式所带来的好处, 在移动代理模式下, 发起者的连接可能很差或是暂时离线的. 看起来唯一的选择好像只能是通过增加一个信任元素来扩展模型了.

这样的一种扩展是使用每个主机上的可信任的和防篡改的硬件模块, 例如智能卡和加密协处理器. 每个硬件模块拥有一个公钥, 使用这样一种架构移动代理可以安全的执行, 具体方式如下: 生成移动代理后, 发起者 H_1 用硬件模块的公钥加密该代理, 收到加密的移动代理后, 主机 H_j ($j>1$) 把它和 H_j 的输入 y_j 一起传递给硬件模块. 模块解密代码, 并在所提供的输入设备上执行它且用 H_{j+1} 上的模块的公钥加密结果, 然后返回加密还有 H_j 的输出 z_j 给主机. 主机发送加密代码和加密数据给序列中的下一个主机.

为了确保保密性, 每个硬件模块必须是可信任的以正确的并且只是一次性的执行相应代码. 进一步, 所有的信任模块都必须由一个可信任外部实体所生产和初始化.

下一部分, 我们介绍一种可选的扩展, 它基于一个最低限度的信任伙伴, 称为可信任服务.

3 移动代理保护模型

3.1 可信任服务

假定存在一个第三方 T, 它是在线的并且和运行代理应用程序的所有主机是相连的, 它的目的是为了保护代理计算. 有没有可能建立这样一种安全的移动计算方案, 其中 T 本身不能获得任何关于计算的信息, 并且所有的计算应该是少交互或非交互的. 我们的答案是肯定的. 下面我们描述具有这样特性的方案, 并且我们假定: (1)T 不与发起者合谋攻击主机, (2)T 不与任何主机合谋攻击发起者或其他主机.

我们扩展了移动代理通讯模式, 增加了两类消息, 从每个主机 H 到发起者的消息, 及从发起者到主机 H 的消息. 图 2给出了传统的移动代理的通讯模式和我们方案中所给出的通讯模式.

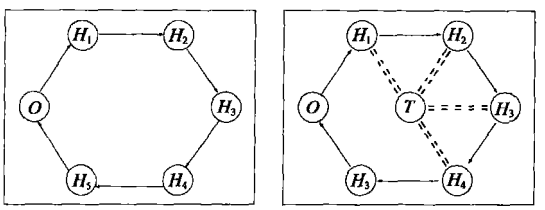

图 2 移动代理通讯模式

我们的技术基于加密一个二元数字电路, 它实现了代理计算中必须维护保密性的部分. 虽然理论上这样的电路适用于任意计算模式, 但对大程序而言, 相关开销却是很大的, 而对于一个代理应用程序的一小部分, 比如购物代理的比较功能, 开销却是可以接受的. 我们首先回顾交互安全协议的加密电路构造器.

3.2 加密电路构造

加密电路构造是一种由两方参与的安全函数计算的交互协议.

我们用一个二元函数 $g(\cdot,\cdot)$ 来描述它, 参与者为 Alice(输入 x)和 Bob(输入 y). Bob收到结果 $z=g(x,y)$, 但对其他一无所知, 而 Alice什么也不知道. 我们给出一个加密电路构造的概要描述:

设 $(x_1,\cdots,x_{n_x})$ $(y_1,\cdots,y_{n_y})$ 和 $(z_1,\cdots,z_{n_z})$ 分别为 x, y 和 z 的二进制表示, 而 C 表示一个多项式尺度的二元电路计算 g. 构造器的基本组件是: (1)一个算法 construct, Alice 用它来构造一个保密电路; (2)Alice 和 Bob之间的传输协议; (3)一个算法 evaluate, 允许 Bob得到 g(x, y). 更详细的步骤如下:

(1)算法 construct(C)以电路作为输入而输出为一个四元组 (C, L, K, U), 其中 C 可以看作 n_x+n_y ——输入电路 C 的加密版本, 而 L、K 以及 U 表示密钥对电路表.

$L=(L_{1,0},L_{1,1}),\cdots,(L_{n_x,0},L_{n_x,1})$

$K=(K_{1,0},K_{1,1}),\cdots,(K_{n_y,0},K_{n_y,1})$

$U=(U_{1,0},U_{1,1}),\cdots,(U_{n_z,0},U_{n_z,1})$

它们分别对应于 x, y 和 z

为了从加密 C 计算出 C(x, y). Bob需要每个输入位的一个密钥: $L_{i,b}$ 对应于输入位 $x_i=b$ 而 $K_{i,b}$ 对应于输入位 $y_i=b$. 密钥 $U_{i,0}$ 和 $U_{i,1}$ 代表加密电路的输出位. 如果计算结果为 $U_{i,b}$ 那么输出位 z_i 就等于 b.

这种精确的方法因为 C 是加密的所以可确保电路中的每个门都给予两个代表输入位的密钥, 而代表输出结果位的密钥可以很容易的计算出, 但是得不到关于它所表示的明文位的任何信息.

(2)Alice 和 Bob采用的一种为“不经意传输”或“秘密的暴露与不暴露”准备的协议. 这是一种交互的两方参与的协议. 其中发送者输入两个消息 m_0 和 m_1 而选择者输入一个位 σ, 最后选择者接收到 m_σ 但是对 $m_{\sigma\oplus 1}$ 一无所知, 而发送者对 σ 一无所知. 更细一步, Alice作为 $K_{i,0}$ 和 $K_{i,1}$ 的发送者而 Bob把 y_i 作为输入值 $K'_i=K_{i,y_i}$ 但不知道 $K_{i,y_i\oplus 1}$. 同时, Alice也不知道 y_i. 另外, 计算表示 x 的密钥值 $L'_i=L_{i,x_i}$, 其中 $i=1,\cdots,n_x$ 并发送

$$C, L'_1,\cdots,L'_{n_x}, U$$

给 Bob.

(3)算法 evaluate$(C, L'_1,\cdots,L'_{n_x}, K'_1,\cdots,K'_{n_y})$ 的输入为加密的电路, 用各自密钥表示的 x 和 y, 结果为密钥 $U'_1,\cdots,U'_{n_z}$. 如果 Alice和 Bob遵循该协议则 Bob可以从中得到 z, 且 $z=g(x,y)$.

3.3 基本模型

我们首先给出如何使用加密电路构造来实现安全的单主机的移动代码计算. 在下一部分考虑扩展到多主机.

假定已经公布了一种加密方案的公钥, 我们用 $E_T(\cdot)$ 和 $D_T(\cdot)$ 分别表示相应的加密和解密操作. 进一步假定所有的参与者都能通过安全的验证电路进行通讯. 这种安全的验证电路可以使用标准的公钥加密和数字签名来实现.

基本思想是 O 构造一个加密电路 C 计算 ξ 和 z 的值它发送 C 给 H, 但是在 K 中为 T 加密所有的密钥 (这不包括 U 中的密钥对, 该密钥对对应于 ξ(用 U_x 表示)), 所以 H 不会知道任何关于 ξ 的事情, 然后 H 从 K 中选择代表 y 的加密密钥并调用 T 在第一轮交互中来解密它们. 随后 H 计算电路并获得 z, 它还会返回电路输出中代表 ξ 的密钥给 O, O 可以从中求出 ξ.

现在给出进一步的细节, 设 C 为二进制电路计算 $(\xi, z) = (g(x, y), h(x, y))$, 从相同的输入 $n_x + n_y$, 输入位为 $x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}$; 和输出 $n_x + n_z$, 输出位为 $\xi_1, \ldots, \xi_{n_x}, Z_1, \ldots, Z_{n_z}$.

对上一部分的符号作一些微小的改动. 这个基本模型经由 5个步骤:

(1)O 选择一个字符串 id 唯一标识计算等, 包括 O 的名字, g 和 h 的描述及一个序列号, O 调用 construct(C) 并得到 U 关联的 (C, L, K, U), 总共由 $n_x + n_z$ 对密钥对组成. 我们用 U_x 表示 U 中的密钥对 $1, \ldots, n_x$, 用 U_z 表示另外的密钥对 $n_x + 1, \ldots, n_x + n_z$;

对 $i = 1, \ldots, n_y$ 及 $b \in \{0, 1\}$, 计算

$$\overline{K}_{i,b} = E_T(id \| i \| K_{i,b})$$

用 $\overline{K}$ 表示所有这些 $\overline{K}$ 的密钥对的列表. 则 O 令如上 $L'_i = L_{i,x_i}$ 其中 x_i ($i = 1, \ldots, n_x$) 并发送

$$id, C, L'_1, \ldots, L'_{nx}, \overline{K}, U_z$$

给 H.

(2)H 令 $\overline{K}'_i = \overline{K}_{i,y_i}$ (其中 $i = 1, \ldots, n_y$) 为代表它的输入 y 的加密并发送它们给 T (加上 id).

(3)T 解密 $\overline{K}'_i$ (其中 $i = 1, \ldots, n_y$) 并验证第 i 个解密字符串是否包含标识 id 和索引 i; 如果所有检查是成功的, T 返回解密密钥 $K'_1, \ldots, K'_{n_y}$ 给 H.

(4)H 调用 evaluate$(C, L'_1, \ldots, L'_{nx}, K'_1, \ldots, K'_{n_y})$ 得到 $U'_1, \ldots, U'_{nx+n_z}$, 然后 H 求出 $z = (z_1, \ldots, z_{nz})$, 从而 $U_{nx+i}, z_i) = U'_{nx+i}$, (其中 $i = 1, \ldots, n_z$) 并转发剩余值 $U'_1, \ldots, U'_{n_x}$ 给 O

(5)O 求出它的输出 $\xi = (\xi_1, \ldots, \xi_{nx})$ 而 $U_{i,\xi_i} = U'_i$, 其中 $i = 1, \ldots, n_x$.

这是一种基本模型, 它工作的前提是假定所有的参与者遵循该协议.

该模型与它原始的加密电路构造一样安全. 假定 T 用的公钥加密是语义安全的并且 T 没有和 H 或 O 串通好, 更准确的说, 对发起者 O 和主机 H, 它们直接对应于加密电路构造方法; 就其本身而言, T 并不能得到关于电路的任何有用信息, 它只看到随机密钥, 但如果 T 和 O 串通, 在任何 T 和 O 串通的地方它们就会知道 H 的输入, 有了 H 的几个不同输入值就可以计算电路了, 也就能得到关于 O 的输入的信息.

为了避免协议偏差使得该模型具有鲁棒性, 必须进行一些额外的步骤; 这需要每个参与者的证明 (可以使用零知识证明), 证明它们根据协议正确进行了所有的操作. T 必须使用一个公钥系统, 这是安全抵御自适应性选择密码攻击的方法, O 和 H 必须对它们的输入负责, 在一个实际系统中, 所有的这些可以用一种 "随机 oracle 模型" (使用一个安全的哈希函数) 实现. 在本模型中, 公钥加密方案和电路加密的伪随机函数必须被实现.

3.4 模型进一步扩展

我们扩展上述模型, 来阐述一个一般性的移动计算保护模型, 一般性是指这是基于 2 1部分的模型即有 $H_1, H_2, \ldots, H_l$ 个主机参与其中的, 每个主机执行上述基本方案的 2 – 4 并发送代理到下一个主机.

发起者必须为每个主机准备一个加密电路, 并且有方法来处理加密态 x_{j-1} 从 $C^{(j-1)}$ 到 $C^{(j)}$ ($j > 1$), 这可以用来自 $C^{(j-1)}$ 的输出密钥 $U'^{(j-1)}_1, \ldots, U'^{(j-1)}_{n_z}$ 来解密一个的隐藏输入到 $C^{(j)}$.

假定存在一个语义的加密系统, 在密钥 K 下, 加密和解密操作分别用 $E_k(\cdot)$ 和 $D_k(\cdot)$ 表示, 加密系统必须包含足够的冗余性, 以给出一个私有密钥 U 和一个加密明文 c, 可用于判断 c 是不是 U 下的一个加密.

修改后的模型如下所示:

(1)O 以对 C 同样的方式得到 $C^{(j)}, L^{(j)}, K^{(j)}, U^{(j)}$ 和 $\overline{K}^{(j)}$ ($j = 1, \ldots, l$), 但是, 它只为 $C^{(1)}$ 选择值 $L'_i = L^{(1)}_{i,x_i}$. 第 j 个标识为 id ‖ j, 发起者还准备好两个加密:

$$E_{U^{(j)}_{i,0}}(L^{(j)}_{i,0}) \text{和} E_{U^{(j)}_{i,1}}(L^{(j)}_{i,1})\, id$$

(其中 $j > 2$, $i = 1, \ldots, n_x$) 并且在将它们赋值给 $V^{(j)}_{i,0}$ 和 $V^{(j)}_{i,1}$ 之前随机置换它们; 调用这样的密钥对 $V^{(j)}$ 后, O 在一个消息中发送 $id, L'_1, \ldots, L'_{nx}, C^{(1)}, \overline{K}^{(1)}, U^{(1)}_z$ 以及 $C^{(j)}, \overline{K}^{(j)}, U^{(j)}_z, V^{(j)}$ (其中 $j = 2, \ldots, l$) 给 H_1.

(2)对每个 $j > 1$, 当 H_j 运行基本模型的第二步时, 它已经从 H_{j-1} (先前计算 $C^{(j-1)}$ 的) 收到 $V^{(j)}$ 和 $U'^{(j-1)}_1, \ldots, U'^{(j-1)}_{nx}$. 主机解析每个 $U'^{(j-1)}_i$ 作为 E 的一个语义密钥, 来判断它解密的是 $V^{(j)}_{i,0}$ 和 $V^{(j)}_{i,1}$ 中的哪一个密文, 然后解密所匹配的那一个. 这就产生 K^j_i, 移动代理当前状态 x_j 的第 i 位的不经意表示. 这些密钥后面被用来计算 $C^{(j)}$.

(3)当 H_j 已经得到计算 $C^{(j)}$ 的结果后, 它转发从 H_{j-1} 收到的所有结果连同 $U'^{(j)}_1, \ldots, U'^{(j)}_{nz}$ 给 H_{j+1}. 在循环的最后, H_l 仅返回 $U'^{(l)}_i$ 给 O.

4 应用实例分析

在我们构造的安全基本模型和扩展模型基础上以一个实例来阐明其应用. 我们假定一个客户需要购买一个商品, 他要访问几个商家的站点并且比较商品, 不仅仅是根据价格还包括其他因素, 然后来选择自己满意的商品. 在这里客户要维护自己的隐私, 而商家对购买者的策略和其他商家的信息比较感兴趣, 客户如何保密这些信息的同时向商家提供必要信息. 另外, 对一些价格是对个人定制的企业, 例如保险业, 商家也需要使计算价格的方法是保密的. 所有这些都可以借助上述的安全代理计算模型来实现.

情形 1: 我们先来分析客户和一个商家之间的谈判, 商家发送一个代理给购买者. 所涉及的角色如表 1所示. 在可信任服务的帮助下, 此代理向购买者提供商品信息, 商家也得到买家的一些反馈信息, 并且他申明对买家信息保密. 由于借助于可信任服务, 买家和商家都只能获得既定的结果信息, 并且任何行为都可以得到验证(比如透露个人隐私).

表 1 参与谈判的角色

O	某商家
H	客户
T	可信任服务

我们来说明具体过程, 如前所述, 我们假定 O、T 及 H 之间的通信是安全的, 问题的焦点关注代理是否受到攻击, 为简单起见, 我们只简略说明这个过程, 如图 3所示.

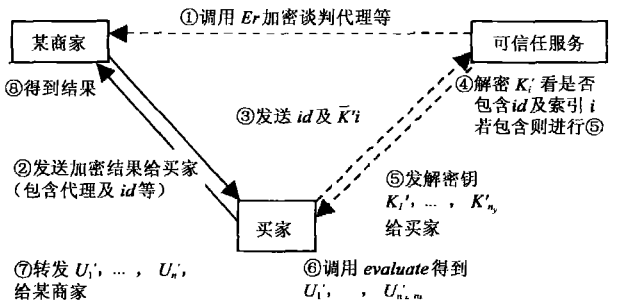

图 3 谈判代理交互过程

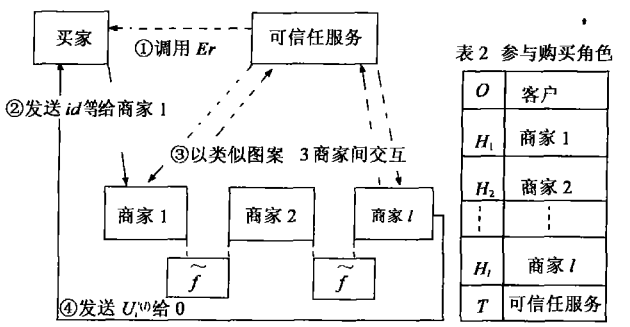

表 2 参与购买角色

O	客户
H_1	商家 1
H_2	商家 2
⋮	⋮
H_l	商家 l
T	可信任服务

图 4 购买代理交互过程

情形 2 一个购物代理出发并从多个商家搜集商品信息这时可使用扩展的安全计算模型了, 所对应的角色如表 2所示. 代理按照某种次序访问多个地址得到相应的商品信息除此以外它一无所获, 而商家可以获得买家的隐私, 前提是他必须承诺不透露个人信息. 因为该交互过程包含了许多如图 3所示的步骤(O 和 H 的角色不同)所以不妨定义一个功能体 $\tilde{f}$ 表示形如图 3的交互过程, 则, 一个购买交互过程可以简单的描述如图 4所示.

在图 4中, 我们简化了描述, 具体请对照模型描述. 同样我们也假定 O、T 及 H 之间的通信是安全的.

5 结束语

本文主要讨论移动代理技术中存在的安全问题, 我们在分析现有的基于"加密函数"方法不足的基础上提出基于加密电路构造协议的模型, 我们引入一个第三方元素称为可信任服务, 阐述了具体运作步骤. 基于高级密码学的移动代理保护是一个好的思路, 下一步我们探讨高级密码协议在移动代理环境中的具体实施和应用以期达到低成本高效率保护移动代理的目的.

参考文献:

[1] 王汝传. 移动代理安全机制的研究[J]. 计算机学报, 2002, 25(12): 1294-1301.

[2] Greenberg M S, Byington J C, Harper D G. Mobile agents and security[J]. Communications Magazine, IEEE, 1998, 36(7): 76-85.

[3] Micali S, Rogaway P. Secure computation[A]. Advances in Cryptology: CRYPTO 91[C]. Lecture Notes in Computer Science, 1992, 576: 392-404.

[4] 王汝传, 孙开翠, 张登银, 杨立扬. 基于 JavaCard 的移动代理保护的研究[J]. 计算机学报, 2004, 27(4): 492-499.

[5] Wilhelm U G, Staamann S, Buttyan L. Introducing trusted third parties to the mobile agent paradigm[A]. Secure Internet Programming[C]. Lecture Notes in Computer Science, col 1603, Springer, 1999. 469-589.

[6] Yao A C. How to generate and exchange secrets[A]. Proc 27th IEEE Symposium on Fundations of Computer Science[C]. 1986. 162-167.

[7] Yee B. A sanctuary for mobile agents[A]. Secure Internet Programming[C]. Lecture Notes in Computer Science, Springer, 1999, 1603. 261-273.

作者简介:

郑 彦 男, 1957年生于南京, 南京邮电大学计算机学院副教授, 博士. 主要研究方向为数据挖掘、信息安全以及移动代理等.

王汝传 男, 1943年生于安徽合肥, 教授、博士生导师. 主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等. E-mail: wangr@njupt.edu.cn

穆 鸿 男, 1980年生于江苏盐城, 博士研究生. 主要研究方向为计算机网络、移动代理和信息安全技术.

王海艳 女, 1974年生于江苏扬州, 南京邮电大学计算机学院讲师, 博士生. 主要研究方向为计算机软件、计算机网络、信息安全、移动代理等.