一个匿名 Internet 移动代理方案

王常杰, 张方国, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 移动代理技术是一种新兴的网络技术, 而电子商务是移动代理技术的主要应用之一. 在本文中, 我们针对电子商务中对用户的匿名性有较高要求的问题, 设计了一个适用于电子商务的匿名 Internet 移动代理方案. 在本方案中, 服务器可以验证每个移动代理程序的身份的有效性, 但不能确认该代理程序的具体身份, 而对服务器进行恶意攻击的代理程序可由代理管理中心进行追踪.

关键词: 移动代理; 电子商务; 匿名性; 一次性数字签字
中图分类号: TN911 文献标识码: A 文章编号: 0372-2112 (2002) 04-0464-03

An Anonymous Internet Mobile Agent Scheme

WANG Chang-jie, ZHANG Fang-guo, WANG Yu-min
(*National Key Lab. on ISN, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract: Mobile agent technique is a new kind of network technology and the electronic commerce is one of the main applications of mobile agent. In this paper we propose an anonymous mobile agent scheme for Internet applications due to the higher anonymity request of users in electronic commerce. In our scheme, the validity of a mobile agent can be verified by servers without leaking the identity information of user. However, the identity of one whose agent makes a malicious attack to a server will be traced out by Agent Management Center.

Key words: mobile agent; electronic commerce; anonymity and one-off digital signature

1 引言

随着 Internet/ Intranet/ Extranet 的迅速发展, 网络的开放性、共享性和互联程度不断扩大, 许多新的基于 Internet 的应用涌现出来, 而基于 Internet 的电子商务更是发展迅速, WWW (World Wide Web) 也已广泛被采用作为实现信息发布、电子商务以及各种娱乐等的业务平台, 对应于此, 一种新的适用于 Internet 电子商务的网络技术——移动代理技术(Mobile Agent) 也成为目前研究的热点. 移动代理是一种可以在分布式系统中(如计算机网络之间) 自动漫游的代理软件, 在网络不同的节点上, 移动代理可以代表用户的身份与该主机或服务器进行一些交互式计算或其他工作. 与传统的客户-服务器通信模式相比, 移动代理技术是一种更适合于异类网络的通信模式, 其特点与优点在文献[1]中有详细介绍.

电子商务的相关应用是目前移动代理技术最重要的网络应用之一. 基于移动代理技术的电子商务涉及很多应用领域, 在 Internet 环境下, 一个代理程序可以代表一个网络用户的身份, 与其他代理或服务器进行商业交互, 包括合同协商, 在线拍卖, 商品价格查询以及动态股票检测等等. 一个移动代理的电子商务应用最典型的例子如下: 一个代理程序携带用户的购物信息(如: 货物类型, 价格要求等), 在不同的购物网站之间漫游, 与每个网站服务器之间进行交互查询, 最终返回给用户最佳的商品信息(如: 最便宜的价格), 或直接代表用户与该网站进行交易.

目前, 阻碍移动代理的电子商务发展的最大障碍就是安全问题, 这是由于代理程序是在不同的主机上运行, 因此带来的对主机及对代理程序的安全威胁就更多. 目前考虑最多的安全问题是如何保护主机免恶意代理程序的攻击(此类攻击如: 非法授权资源接入、对服务器的业务拒绝攻击以及伪装其他合法代理程序欺骗服务器等) 以及如何保护代理程序免受恶意主机的攻击(此类攻击如: 篡改代理程序代码或信息、偷窃代理程序的信息等), 针对以上的安全问题, 一些安全解决方案[2~4]已经提出. 但是, 目前几乎所有的安全移动代理系统都没有考虑到对移动代理程序的匿名性问题, 即: 在与不同的服务器交互时, 代理程序的身份(即所代表的用户) 都是公开的(服务器必须验证代理程序的合法身份, 才能允许代理程序的运行), 我们知道, 在电子商务中, 用户的匿名性是安全性考虑的一个重要方面, 如电子现金的匿名性[5]要求等, 而由于移动代理程序的非匿名性将影响电子现金的匿名性(即服务器可以通过确认某个移动代理程序的身份, 将相应的电子交易中的电子现金与用户身份联系起来), 进而在电子交易中将泄

收稿日期: 2000-11-03; 修回日期: 2001-06-26
基金项目: 国家自然科学基金重大项目(No. 19931010); 国防重点实验室项目(2000JS06.3.1DZ0115)

露用户的身份.

在本文中, 我们设计了一个一次性密钥数字签名方案, 并构造了一个适用于电子商务的匿名 Internet 移动代理方案. 在该方案中, 服务器可以验证每个移动代理程序的身份的有效性, 但不能确认该代理程序的具体身份, 从而实现了匿名性, 同时, 如果某个代理程序对服务器进行了攻击, 该服务器通过向代理管理中心(AMC) 提交相应的签字数据, 由代理管理中心确定该恶意代理程序的发出人, 由其承担相应的责任. 需要指出的是, 在本文中, 我们只考虑了移动代理的匿名性, 该技术可与其他已有的移动代理的安全技术一起使用, 构造完善的安全移动代理系统.

2　方案实现

在本节, 首先给出本方案的实现模型, 然后给出具体的方案实现步骤, 为了实现移动代理程序的匿名性, 在文献[6]的基础上设计了一个基于椭圆曲线的一次性密钥对数字签名, 与原方案相比, 我们的方案是基于椭圆曲线有限点构成的群, 其所需的密钥长度和计算量要小的多, 因此更适用于 Internet 的环境下. 在以下匿名代理方案的具体实现中, 我们将给出详细介绍.

在本方案中, 考虑整个模型由四部分组成, 即用户代理平台、代理管理中心、移动代理程序以及各网络节点(即支持移动代理的Web服务器), 如图 1 所示

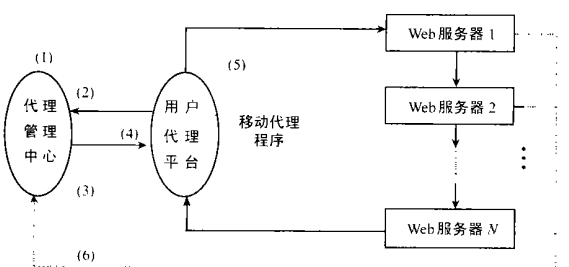

图 1　匿名移动代理方案工作流程

下面, 给出方案的具体实现步骤:

第 **1** 步　系统初始化. 该步骤由代理管理中心(AMC) 完成, AMC 将产生如下的系统参数: 设 p 是大素数, a, $b \in GF(p)$ 满足 $4a^3+27b^2 \neq 0$. 椭圆曲线 $E_{(a,b)}(GF(p))$ 定义为满足方程 $y^2 = x^3 + ax + b$ 的点 $(x, y) \in GF(p) \times GF(p)$ 和特殊点 O(称为无穷远点)所组成的集合. 这些点构成一个 *Abelian* 群. G 是 $E_{(a,b)}(GF(p))$ 中的一个 q 阶元素, q 是一个至少为 160 比特的素数. $R_x(A)$ 是表示取 A 点的 x- 坐标. 有关椭圆曲线的更详细的资料可参看文献[7, 8]. H 是一个单向 Hash 函数, $H: \{0,1\}^* \rightarrow \{0,1\}^k$ ($k \approx 160$), 记号 $(\cdot \| \cdot)$ 是表示两个比特串联接. AMC 将随机选择 $X_{AMC} \in GF(q)^*$ 作为自己的私钥, $P_{AMC} = X_{AMC}G = (x_P, y_P)$ 是公钥, 然后公开 $(E_{(a,b)}(GF(p)), G, q, P_{AMC}, H)$.

第 **2**、**3** 步　用户注册. 即用户代理平台向 AMC 进行注册, 注册结束后, AMC 将拥有该用户的相关身份信息, 但并不知道用户的私钥, 同时用户也得到了 AMC 发给他的可以证明已经注册过的合法数字证书. 注册协议如下:

用户平台 U　　代理管理中心

选择私钥 $X \in {}_RGF(q)^*$,

计算 $Y = XG$　$\xrightarrow{Y,\ ID_U}$　选 $w_U \in {}_RGF(q)^*$, $A_U = w_UG - Y$

$\gamma_U = H(x_p \| y_p) w_U + R_x(A_U) X_{AMC} \bmod q$

$\xrightarrow{(A_U,\ \gamma_U)}$　将 $(A_U, \gamma_U, Y, ID_U, w_U)$ 存入数据库

用户平台 U 首先验证

$$\gamma_U G = H(x_P \| y_P)(A_U + Y) + R_x(A_U) P_{AMC}$$

用户平台注册完成后, 用户 U 从 AMC 获得证书 (A_U, γ_U).

第 **4** 步　移动代理的签字产生. 在该步骤中, 用户代理平台根据用户的要求, 发布移动代理程序. 为隐匿代理程序的身份, 用户平台首先为该代理程序产生一个一次性的密钥对, 然后使用一次性的私钥对该代理的代码、初状态、数据区以及该代理程序的有效时戳等数据进行签字, 过程实现如下:

一次性密钥对的产生:

用户选择一次性私钥 $x_U \in {}_RGF(q)^*$, 计算一次性公钥 $Y_U = x_UG$,

选择 $\phi \in {}_RGF(q)^*$, 计算 $T = \phi G$, $(R_x(T) = t \neq 0 \bmod q$, 否则重选 $\phi)$

$$\alpha = A_U + T,\ \beta = t\alpha,\ Z = tR_x(A_U) \bmod q$$

$$\lambda = \gamma_U t + (\phi t - x_U t + x_U) H(x_P \| y_P) \bmod q$$

至此, 用户平台为其移动代理程序产生一个一次性密钥对 (x_U, Y_U), 和一个证明其身份合法(即已在 AMC 处注册) 的虚拟证书 $VCert: \{Y_U, \alpha, \beta, Z, \lambda\}$.

对移动代理程序的签字:

用户代理平台用一次性私钥对将要发出的移动代理程序的所有初始数据 M (包括该代理的代码、初状态、数据区、路由表、时戳等)进行签字:

选择: $k \in {}_RGF(q)^*$, 计算 $K = kG$, $(R_x(K) \neq 0 \bmod q$, 否则重选 $k)$

计算 $r = H(M) k + R_x(K) x_U \bmod q$, 得到签字信息 $Sig: \{k, r\}$ 后, 将 Sig, $VCert$ 分别与代理程序级连起来. 在签字完成后, 一次性私钥 x_U 不再需要, 为安全起见, 可由用户平台将其删除. 完成签字以后, 移动代理程序的结构如下:

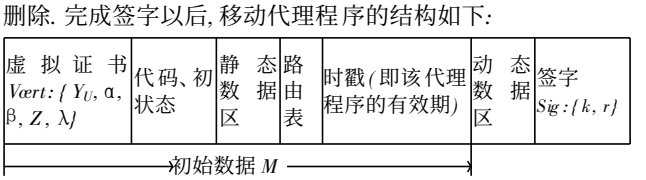

图 2　签字后匿名移动代理的结构

第 **5** 步　服务器效验代理程序.

携带签字信息的移动代理程序依照路由表在 Web 服务器 1 到 Web 服务器 N 之间进行漫游, 在每个服务器上运行并与每个服务器进行交互, 最终完成任务(如: 以最低的价格完成购物). 首先, 服务器将验证该代理程序的身份(包括验证虚拟证书和验证一次性私钥的数字签字), 即验证如下等式是否成立:

$$\lambda G = H(x_P \| y_P)(\beta + Y_U) + zP_{AMC}$$　(验证虚拟证书)

$rG = H(M)K + R_x(K)\,Y_U$ (验证一次性私钥的数字签字)

若等式成立,则服务器验证该移动代理程序身份合法,并给予相应的资源接入权限并记录该代理的 *Vcert* 和 *Sig*. 若验证不通过,服务器则拒绝执行该代理程序,并做相应的日志. 需要指出的是,服务器只能验证代理程序的合法性,但无法从以上两式得到该代理身份的任何信息.

第 **6** 步 恶意代理的追踪.

当服务器发现在其主机上运行的某个代理程序有恶意行为(如:攻击服务器或其他代理)时,服务器提交所记录的该代理程序的 *Vcert* 和 *Sig* 给 AMC,以确认该代理的身份(即确定实际用户的身份).

当收到某个服务器提交的恶意代理的投诉及相应的数据($Vcert$ 和 Sig),AMC 的工作如下:

首先验证:$\lambda_G = H(x_P \| y_P)(\beta + Y_U) + zP_{AMC}$ 以确定该代理程序是否注册过. 然后对数据库中的每一记录 $(A_i, Y_i, Y_i, ID_i, w_i)$,验证 $\beta \stackrel{?}{=} (z/R_x(A_i))\,\alpha$ 即 $(Z/R_x(A_U)) = (tR_x(A_U)) * \alpha/R_x(A_U)) = t\alpha = \beta$,若满足,则从 ID_i 可确定出该恶意代理的真实身份(即用户的具体身份).

3 性能分析

在本文中,我们设计的方案主要基于一个一次性密钥对的数字签字,其安全性是基于椭圆曲线离散对数问题(ECDLP),假设 ECDLP 是计算困难的. 下面,给出较为详细的性能分析.

合法移动代理程序的匿名性:在我们的方案中,用户平台为每个将要发布的移动代理程序产生一个一次性的虚拟证书和公私钥对,并用一次性私钥对该代理签字,Web 服务器可以验证每个代理的虚拟证书,但无法确定该代理的具体身份(即所代表的用户),由 $VCert: \{Y_U, \alpha, \beta, \lambda\}$ 恢复用户证书 $\{A_U, Y_U\}$ 的难度相当于计算椭圆曲线离散对数问题.

代理程序匿名性的可撤消:当需要时(如:某移动代理程序有攻击行为),代理的匿名性可由 AMC 撤消. 这种撤消是有条件的,即某 Web 服务器提供足够的证据证明某个移动代理程序有攻击行为,并提供给 AMC 该代理的相应的签字数据.

代理程序签字的不可伪造性:在我们的方案中,任何一方(包括 AMC)都不能模仿一个用户平台的身份签字,从而产生一个代表其身份的移动代理程序,这种攻击的难度相当于破解 AMC 或某用户平台的私钥. 另外,由于用户平台每次产生的一次性私钥 x_U 在签字后即被销毁,因此 x_U 泄露的可能极小,而由 Y_U 推出 x_U 的难度相当于计算 ECDLP.

4 结论

将移动代理技术应用于电子商务领域的一个急需解决的问题就是移动代理系统的安全问题. 在本文中,我们针对电子商务中对用户匿名性的要求,设计了一个适用于电子商务的 Internet 匿名代理方案. 本方案具有如下特点:第一,用户每次发布的移动代理程序都采用一次性虚拟证书和一次性公私钥对进行签字,任何 Web 服务器只能验证代理程序的合法性,但无法确认代理程序的身份(即用户身份). 第二,对于恶意代理程序,可由代理管理中心,追踪其身份. 第三,本方案是基于椭圆曲线离散对数问题,其所需的数据量(包括代理程序携带的数据量,以及与 Web 服务器交互验证的数据量)远小于实现同等安全强度的离散对数体制,因此,本方案非常实用.

参考文献:

[1] Danny B Lange, Mitsuru Oshima. Seven good reasons for mobile agents [J]. Communications of ACM, 1999, 42(3): 88-89.

[2] IBM, Inc. IBM aglets documentation web page [EB/OL]. http://aglets.trl.ibm.co.jp/documentation.html, 1998.

[3] Concordia: Java Mobile Agent Technology [EB/OL]. http://www.meitca.com/HSL/Projects/Concordia/, 1998.

[4] Robert S Gray. Agent Tcl: A flexible and secure mobile-agent system [A]. Proc of the Fourth Annual Tcl/Tk Workshop (TCL'96) [C]. California: Monterey, 1996.9-23.

[5] J Claessens, B Preneel, J Vandewalle. Anonymity controlled electronic payment systems [A]. Proceedings of the 20th symposium on information theory in the benclux [C]. Belgium: Haasrode, 1999.109-116.

[6] X Yi, C K Siwe, M R Syed. Digital signaature with one-time pair of keys [J]. IEE Electronics Letters, 2000, 36(2): 130-131.

[7] V S Miller. Use of Elliptic Curve in Cryptography [A]. In Advances in Cryptology-CRYPTO'85 [C]. California: Santa Barbara, Spring-Verlag, 1985.417-426.

[8] N Koblitz. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(2): 203-209.

作者简介:

王常杰 男,1974 年 9 月出生于江苏南京,1999 年 3 月获西安电子科技大学通信与信息系统硕士学位,现为西安电子科技大学在读博士,已发表论文数篇,研究方向为网络安全与电子商务.

张方国 男,1972 年 12 月出生,1999 年 3 月在上海同济大学应用数学系获得理学硕士学位,现在西安电子科技大学通信工程学院攻读密码学博士学位,已发表论文数篇,研究兴趣是椭圆曲线密码体制和超椭圆曲线密码体制及电子商务.

王育民 男,1936 年生,教授,IEEE 高级会员,博士生导师,长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究;Tel: 029-8201016; Email: ymwang@xidian.edu.cn