一种新的移动代理路由解决方案

柳毅¹ 丁勇² 庞辽军³

(广东工业大学计算机学院 广州 510006)¹ (桂林电子科技大学数学与计算科学学院 桂林 541004)²
(西安电子科技大学综合业务网国家重点实验室 西安 710071)³

摘要 移动代理是一种软件程序,它漫游在计算机网络中,经过不同的主机代替用户执行一定的任务,但是它也带来了许多新的有关面临恶意代理与安全的问题。对已有的移动代理路由协议进行了分析讨论,在此基础上,利用一种满足结合律但不满足交换律的单向函数,构造了一种新的移动代理路由解决方案,并对其安全性和计算复杂度进行了详细分析。结果表明,该协议满足路由协议的所有安全性质,而且具有更低的计算复杂度。

关键词 移动代理,单向函数,计算复杂度

中图分类号 TN915.08 **文献标识码** A

Secure Itinerary Protection Based on Mobile Agents

LIU Yi¹ DING Yong² PANG Liao-jun³

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)¹
(School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin 541004, China)²
(National Key Laboratory on Integrated Services Networks, Xidian University, Xi'an 710071, China)³

Abstract Mobile agents are software programs that can be autonomously migrated from host to host to fulfill their goals. It also creates significant new security threats from malicious agents and hosts. Route protection is one of them. It is important to protect the routes of a mobile agent if it will visit a list hosts or if it will dispatch some mobile agents to other hosts. Route protections available were analyzed and discussed. After that, a new mobile agents route protection was given using non-commutative associative one-way functions. The analysis shows that this method not only satisfies a set of general security properties for agent route protection, but also has lower computational cost than those existed.

Keywords Mobile agents, One-way functions, Computational cost

1 引言

移动代理是一个代替用户或其它程序执行某种任务的程序,能在异构网络的不同主机间自主地迁移,并可与其他代理或资源进行交互,是一种适应大型异构网络(如 Internet)的分布计算模型。移动代理“迁移-计算-迁移”的工作模式以及代理间的通信和协作能力为分布应用提供了全新的整体解决方案。而且以上这些特点都是网络技术开发中所需要的,因此得到了极大的关注。在分布式应用中,其优点不言而喻。

然而,由于代理的移动特点,也带来了许多新的安全问题^[1]。针对移动代理的路由问题,文献[2-6]提出了一系列的移动代理路由方案。通过文献[7]的分析比较指出,其中满足安全路由性质的协议只有文献[4-6];而在计算复杂度方面,文献[7]的方案最优。但文献[6]中,为了保证代理路由的安全性,用户在每次派发移动代理时,都需要产生大量的一次性随机数,而以往产生的随机数不能重复使用,这给需要经常多次派发移动代理的用户带来很大的不便。

本文利用一种满足结合律但不满足交换律的单向函数,构造一种新的移动代理路由解决方案。方案对于派发代理的用户来说,即使多次派发代理,也不需要多次产生相关数据,只需要更新一个随机数,其余数据可以多次重复使用,并不会带来安全问题。而且方案相比文献[6]进一步降低了计算复杂度。

2 移动代理路由协议的安全性质

关于移动代理路由,文献[2,3]提出安全的移动代理路由应该满足以下几条性质:

P1)防修改。恶意主机不能擅自修改代理路由,即使它们相互勾结也不能达到目的。

P2)信息最小泄露。路由上的任意主机仅知道它的先驱者和后继者,路由上其他主机的信息对它来说是不可知的。

P3)可证实性。路由上的任意主机都能证实它是代理路由的一部分。

P4)代理来源确认性。路由上的每一主机都能确认代理

到稿日期:2008-12-09 返修日期:2009-03-05 本文受国家自然科学基金(60803151),广东联合基金重点项目(U0835004),广东工业大学博士启动基金(073036)资助。

柳毅(1976-),男,博士后,副教授,主要研究方向为密码学与信息安全,E-mail:liuyi_xd@126.com;丁勇(1975-),男,博士后,副教授,主要研究方向为密码学与信息安全;庞辽军(1977-),男,博士后,副教授,主要研究方向为密码学与信息安全。

确实来自于它的先驱主机。

P5)具有时戳性。代理路由不会被恶意主机进行重放攻击。

3 单向函数

本文采用的单向函数 f 定义如下(更详细的定义参见文献[9]):

设 Σ^* 为 0,1 比特串, f 为 $\Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ 的一个映射函数,具有下列性质:

1)可计算性。函数 f 是多项式时间可计算的,当且仅当存在一个多项式 p ,对于所有的 $a, b \in \Sigma^*$, $f(a, b)$ 的计算时间上界为 $p(|a| + |b|)$ 。其中 $|x|$ 为比特串 x 的长度。

2)强不可逆性。给定任意的 $c = f(a, b)$ 和 a , 找到 $\hat{b}$ 满足 $c = f(a, \hat{b})$ 的概率可以忽略不计;或者给定任意的 $c = f(a, b)$ 和 b , 找到 $\hat{a}$ 满足 $c = f(\hat{a}, b)$ 的概率可以忽略不计。

3)结合律。函数 σ 满足结合律,当且仅当对于所有的 $a, b, c \in \Sigma^*$, 存在 $f(f(a, b), c) = f(a, f(b, c))$ 。

4)非交换律。对于任意的 $a, b \in \Sigma^*$, 以很大的概率满足 $f(a, b) \neq f(b, a)$, 即等式成立的概率可以忽略不计。

4 一种新的移动代理路由解决方案

4.1 符号标记

路由协议中一些符号标记如下。

H_0 : 移动代理主人(用户)的 IP 地址;

H_i : 移动代理路由经过的第 i 个主机的 IP 地址;

PK_i : H_i 的公钥;

$S_i(m)$: 用 H_i 的私钥对消息 m 进行签字(如采用 RSA 签名);

$E_{PK_i}(m)$: 用 H_i 的公钥对消息 m 进行加密(如采用 RSA 加密);

$h(\cdot)$: 单向抗碰撞的安全 hash 函数;

f : 上一节定义的单向函数;

t : 时戳。

4.2 新的路由解决方案

(1)初始化

设移动代理在网络中漫游,需要路由经过 n 个主机。用户 H_0 首先生成一条公开信息 m , 产生一个一次性随机数 u , 计算 $v = f(m, u)$, 公开 m 和 v 。每个 $H_i, i=0, 1, \dots, n$ 生成一个秘密比特串 x_i 和一个公开比特串 a_i , 并计算 $y_i = f(x_i, a_i)$, 公开 a_i 和 y_i 。

在代理出发前,用户 H_0 计算

$$\omega_0 = y_0$$

$$\omega_i = f(\omega_{i-1}, y_i), i > 0$$

$$z_0 = f(u, x_0)$$

(2)计算路由 r

$$r = S_0(z_0, t) || E_{PK_1}[H_2, S_0(H_0, H_1, H_2, \omega_0, h_1, t) ||$$

$$E_{PK_2}[H_3, S_0(H_1, H_2, H_3, \omega_1, h_2, t) ||$$

⋮

$$E_{PK_n}[H_0, S_0(H_{n-1}, H_n, H_0, \omega_{n-1}, t)]$$

其中, h_i 表示对主机 H_i 后的所有路由信息进行杂凑后的结果, 即 $h_i = h(E_{PK_{i+1}}[\dots] || \dots || E_{PK_n}[\dots]), i=1, 2, \dots, n-1$ 。

(3)移动代理的漫游

H_1 收到 r 后,首先验证第一部分 H_0 的签名,从 $S_0(z_0, t)$ 中得到 z_0 。接着, H_1 对 r 的第二部分进行解密,知道它的后继主机为 H_2 。通过用户 H_0 的公钥, H_1 能够证实 H_0, H_1 和 H_2 都包含在路由中,并且得到 ω_0 。比较 h_1 与其后路由信息的杂凑值来检查其后路由信息是否被修改。然后,利用公开的 m, a_0, v , 由 H_1 证实以下等式成立:

$$f(f(m, z_0), a_0) = f(v, \omega_0) \quad (1)$$

若一切证实合法, H_1 计算 $z_1 = f(f(z_0, a_0), x_1)$, 把路由信息

$$r_1 = S_1(z_1, t) || E_{PK_2}[H_3, S_0(H_1, H_2, H_3, \omega_1, h_2, t) ||$$

⋮

$$E_{PK_n}[H_0, S_0(H_{n-1}, H_n, H_0, \omega_{n-1}, t)]$$

发送给 H_2 。当 $H_i (i=2, 3, \dots)$ 收到路由信息

$$r_{i-1} = S_{i-1}(z_{i-1}, t) || E_{PK_i}[H_{i+1}, S_0(H_{i-1}, H_i, H_{i+1},$$

$$\omega_{i-1}, h_i, t) ||$$

⋮

$$E_{PK_n}[H_0, S_0(H_{n-1}, H_n, H_0, \omega_{n-1}, t)]$$

后,首先验证 r_{i-1} 第一部分 H_{i-1} 的签名,从 $S_{i-1}(z_{i-1}, t)$ 中得到 z_{i-1} 。接着, H_i 对 r_{i-1} 的第二部分进行解密,知道它的后继主机为 H_{i+1} 。通过用户 H_0 的公钥, H_i 能够证实 H_0, H_1 和 H_2 都包含在路由中,并且得到 ω_{i-1} 。比较 h_i 与其后路由信息的杂凑值来检查其后路由信息是否被修改。然后,利用公开的 m, a_{i-1}, v , 由 H_i 证实以下等式成立:

$$f(f(m, z_{i-1}), a_{i-1}) = f(v, \omega_{i-1}) \quad (2)$$

若一切证实合法, H_i 计算 $z_i = f(f(z_{i-1}, a_{i-1}), x_i)$, 把路由信息

$$r_i = S_i(z_i, t) || E_{PK_{i+1}}[H_{i+2}, S_0(H_i, H_{i+1}, H_{i+2}, \omega_i,$$

$$h_{i+1}, t) ||$$

⋮

$$E_{PK_n}[H_0, S_0(H_{n-1}, H_n, H_0, \omega_{n-1}, t)]$$

发送给 H_{i+1} 。 H_{i+1} 重复以上过程,直到 H_n 。 H_n 完成证实过程后,计算 $z_n = f(f(z_{n-1}, a_{n-1}), x_n)$, 把 $S_n(z_n, t)$ 传回 H_0 。 H_0 证实以下等式:

$$f(f(m, z_n), a_n) = f(v, \omega_n) \quad (3)$$

若等式成立,则表明代理严格按照路由顺序经过了所有的主机。

4.3 方案安全性分析

首先证明在路由主机诚实的前提下式(1)至式(3)的正确性,即

$$f(f(m, z_i), a_i) = f(v, \omega_i), i=0, 1, \dots \quad (4)$$

证明:采用数学归纳法。

1) 当 $i=0$ 时,

$$\begin{aligned} f(f(m, z_0), a_0) &= f(m, f(z_0, a_0)) = f(m, f(f(u, x_0), \\ & a_0)) = f(m, f(u, f(x_0, a_0))) = f(m, \\ & f(u, y_0)) = f(m, f(u, \omega_0)) = f(f(m, \\ & u), \omega_0) = f(v, \omega_0) \end{aligned}$$

2) 假设当 $i=k-1 (k>0)$ 时等式成立,即

$$f(f(m, z_{k-1}), a_{k-1}) = f(v, \omega_{k-1})$$

那么当 $i=k$ 时,

$$\begin{aligned} f(m, z_k) &= f(m, f(f(z_{k-1}, a_{k-1}), x_k)) = f(m, f(z_{k-1}, f \\ & (a_{k-1}, x_k))) = f(f(m, z_{k-1}), f(a_{k-1}, x_k)) = f \end{aligned}$$

$$(f(f(m, z_{k-1}), a_{k-1}), x_k) = f(f(v, \omega_{k-1}), x_k)$$

$$f(f(m, z_k), a_k) = f(f(f(v, \omega_{k-1}), x_k), a_i) = f(f(v, \omega_{k-1}), f(x_k, a_k)) = f(f(v, \omega_{k-1}), y_k) = f(v, f(\omega_{k-1}, y_k)) = f(v, \omega_k)$$

综合 1)、2) 两点可知, 对于 $\forall i=0, 1, \dots$, 都有以下等式成立:

$$f(f(m, z_i), a_i) = f(v, \omega_i)$$

证明完毕。

下面针对安全性质 P1)–P5) 逐条进行分析:

P1) 这里假设协议中选择的加密和签名算法都是安全可靠的。首先, 单独的恶意主机 H_i 不能随意修改(包括增加和删除)路由信息, 否则其后的诚实主机 H_{i+1} 对路由信息进行杂凑函数验证时会很快发现该非法行为。如果恶意主机 H_i 企图使得移动代理不经过诚实主机 $H_{i+1}, \dots, H_{i+k-1}$, 而直接到达其后面的主机 H_{i+k} 。但由于代理路由不经过 $H_{i+1}, \dots, H_{i+k-1}$, 恶意主机就无法得到 $z_{i+1}, \dots, z_{i+k-1}$, 这样 H_{i+k} 在验证等式(4)时会很快发现异常。如果 H_{i+k} 是诚实的, 它就会很快地向用户 H_0 报告; 即便它也是恶意的, 由于没有 $z_{i+1}, \dots, z_{i+k-1}$, H_{i+k} 需要解决的问题是找到一组 $(\hat{\omega}_{i+k}, \hat{z}_{i+k})$, 使得等式 $f(f(m, z_{i+k}), a_{i+k}) = f(v, \hat{\omega}_{i+k})$ 成立。由于函数 f 的特性, 知道 H_{i+k} 不可能找到这样的 $(\hat{\omega}_{i+k}, \hat{z}_{i+k})$, 则它后面的最近诚实主机仍然会向用户报告异常。因此, 该路由协议可以保护移动代理经过所有的诚实主机, 并且一旦发生路由信息恶意修改, 可以很快被代理经过的距离恶意主机最近的诚实主机发现。

P2) 由于每次用户 H_0 在派发移动代理时都要产生新的随机数 u , 因此路由主机 H_i 每次都会计算新的 z_i 。而且, 如果不知道 x_{i+1} , 获得 z_i 对于 z_{i+1} 的计算没有任何帮助。可见, 主机 $H_i, i=1, 2, \dots$ 除了能知道发送代理给它的先驱主机和它的后继主机外, 并不能获得更多的有用信息; 而对于代理路由外的主机, 则不会得到任何路由信息。

P3) 由协议可以看到, 主机 $H_i, i=1, 2, \dots$ 接受到路由信息后, 通过解密并验证 H_0 的签名信息, 的确能够证实自己是代理路由的一部分。

P4) 主机间所具有的 IP 协议可以使得该性质得到满足。

P5) 路由信息中的时戳 t 可以证实是否发生重放攻击。

4.4 计算复杂度分析

由于单向函数和杂凑函数的计算复杂度远远小于公钥体制, 因此该协议的计算复杂度主要由公钥体制下的计算量来决定。

1) 用户方面: 用户 H_0 计算路由 r 时需要进行签名处理的总计算复杂度为 $n+1$, 而需要进行加密处理的总计算复杂度为 n 。

2) 路由主机方面: 从方案处理过程可以得出, 每一路由主机 $H_i (i=1, 2, \dots, n)$ 只需进行一次基本解密、两次验证签名和一次签名。因此, 路由主机总的计算复杂度为: 签名(基本解密)为 $2n$, 加密(验证签名)为 $2n$ 。

4.5 网络信息传输总量

根据路由方案可以得出不同主机间传输的信息量分别为

$(n+1), n, \dots, 2$ 。网络信息传输总量为

$$(n+1) + n + \dots + 2 = \frac{n(n+1)}{2} + n$$

表 1 为不同路由协议的性能比较。

表 1 路由协议性能比较

路由方案	计算复杂度及信息传输量	用户		路由主机		网络信息传输量
		加密 (验证签名)	签字 (解密)	加密 (验证签名)	签字 (解密)	
文献[4]		$\frac{n(n+1)}{2}$	$\frac{n(n+1)}{2}$	$\frac{n(n+1)}{2}$	$\frac{n(n+1)}{2}$	$2n-1$
文献[5]		$\frac{n(n+1)}{2}$	n	n	$\frac{n(n+1)}{2}$	$\frac{n(n+1)}{2}$
文献[6]		$n+1$	$n+1$	$3n$	$3n$	$\frac{n(n+1)}{2} + n$
本文方案		n	$n+1$	$2n$	$2n$	$\frac{n(n+1)}{2} + n$

结束语 移动代理由于其自身所具有的优异特性, 已经在很多新兴领域得到了应用。但是安全问题一直是移动代理技术得到更广泛应用的一个绊脚石。本文利用一种单向函数, 从新的角度构造了一个移动代理路由安全解决方案。对于需要多次派发代理的用户, 该方案仅需要用户每次更新一个随机数即可, 不需要用户每次产生大量的随机数^[7], 简化了用户的工作, 并且进一步降低了路由主机的计算复杂度。

参考文献

- [1] Perry M, Zhang Q. SITA: Protecting Trade Agents from Malicious Host[A]// Mobile Agents for Telecommunication Applications, LNCS 2164[C]. Springer, 2001: 173-183
- [2] Domingo - Ferrer J. Mobile Agent Route Protection through Hash-based Mechanisms[A]// LNCS 2247[C]. Berlin Heidelberg: Springer-Verlag, 2001: 17-29
- [3] Westhoff D, Schneider M, Unger C, et al. Methods for Protecting a Mobile Agent's Route[A]// ISW'99 LNCS 1729[C]. Berlin Heidelberg: Springer-Verlag, 1999: 57-71
- [4] Westhoff D, Schneider M, Unger C, et al. Protecting a Mobile Agent's Route Against Collusions[A]// LNCS 1758[C]. Berlin Heidelberg: Springer-Verlag, 2000: 215-225
- [5] Mir J, Borrell J. Protecting General Flexible Itineraries of Mobile Agents[A]// ICICS 2001, LNCS 2288[C]. Berlin Heidelberg: Springer-Verlag, 2002: 382-396
- [6] 柳毅, 伍前红, 王育民. 基于移动代理的可变路由安全协议[J]. 计算机学报, 2005, 28(7): 1118-1122
- [7] Cubaleska B, Schneider M. A Method for Protecting Mobile Agents Against Denial of Service Attacks[C]// LNCS 2446. Berlin Heidelberg: Springer-Verlag, 2002: 297-311
- [8] Esparza O, Soriano M, Muñoz J L, et al. A Protocol for Detecting Malicious Hosts Based on Limiting the Execution Time of Mobile Agents[C]// Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC' 2003). 2003
- [9] Hemaspaandra L A, Rothe J, Saxena A. Enforcing and Defying Associativity, Commutativity, Totality, and Strong Noninvertibility for One-way Functions in Complexity Theory[R]. UR CSD 854. University of Rochester, December 2004