一个新的基于Merkle树的移动代理路由解决方案

柳 毅[1,2] 郝彦军[1] 庞辽军[3]
(广东工业大学计算机学院 广州 510006)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[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,被认为在未来的电子商务中将起到很重要的作用。但安全问题一直是移动代理得到实际应用的一个很大障碍。对已有的移动代理路由协议进行了分析讨论,在此基础上,利用一种特殊单向函数,结合Merkle树结构,构造了一个新的基于Merkle树的移动代理路由解决方案。该方案不仅具有更好的使用安全性和便利性,而且具有更低的计算复杂度。

关键词 移动代理,单向函数,Merkle树,计算复杂度
中图法分类号 TN915.08 **文献标识码** A

New Mobile Agents Secure Itinerary Protection Based on Merkle Trees

LIU Yi[1,2] HAO Yan-jun[1] PANG Liao-jun[3]
(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]
(National Key Laboratory on Integrated Services Networks, Xidian University, Xi'an 710071, China)[3]

Abstract Mobile agents are software programs which are believed to play an important role in future e-commerce systems, but the security problems have been an obstacle for mobile agents to be practical. Using a special one-way function and Merkle trees, a route protection of mobile agents was presented in this paper which not only owns better security and convenience but also reduces the computational cost.

Keywords Mobile agents, One-way functions, Merkle trees, 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,它得到了极大的关注。在分布式应用中,其优点不言而喻。

然而,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。其中文献[2]首次将Merkle树的结构引入到移动代理路由协议中,使其具有较低的计算复杂度。然而,我们在文献[6]中曾经指出文献[2]的协议不能抵制主机间的联合攻击,并且给出了一个解决方案。但在该方案中,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,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。

本文通过一种特殊单向函数,构造一个新的基于Merkle树的移动代理路由协议。该协议对于派发代理的用户来说,即使多次派发代理,也只需更新一个随机数,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要求

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:

S1. 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。

S2. 信息的最小泄露: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。

S3. 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。

S4. 代理来源确认性:路由上的每一主机都能确认,代理确实来自于它的先驱主机。

S5. 具有时戳性:代理路由不会被恶意主机进行重放攻击。

到稿日期:2010-06-22 返修日期:2010-09-07 本文受国家自然科学基金(60803151)和计算机软件新技术国家重点实验室开放基金(2010B13)资助。

柳 毅(1976-),男,博士后,副教授,CCF会员,主要研究方向为网络与信息安全,E-mail:liuyi_xd@126.com;郝彦军(1974-),男,博士,讲师,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。

3 Merkle 树

Merkle 树是指这样一种树结构：树的每一个叶结点由一条指令加上该指令的 hash 值构成；每个父结点下面的所有子结点的 hash 值组合到一起，再进行 hash 运算就得到它们的父结点；这个过程一直进行下去，直至得到树的根结点。

路由协议中采用 2-3 元 Merkle 树，即 Merkle 树的每一父结点下包含 2 个或 3 个子结点。采用 2-3 元 Merkle 树是为了保证：对于任意数目的路由主机 $n>1$（$n=1$ 时，即只有一个路由主机的情况比较简单，这里不予考虑），所有主机的路由信息都能包含在 Merkle 树的叶结点中。这是由于对于任意正整数 $n>1$，存在非负整数 k 和 l 使得：$2k+3l=n$。不妨这样选取 k 和 l：当 n 为偶数时，$k=n/2$，$l=0$；当 n 为奇数时，$k=(n-3)/2$，$l=1$。

4 特殊单向函数

本文采用的特殊单向函数 f 定义如下[7]：

设 $\sum^*$ 为 0，1 比特串，f 为 $\sum^* \times \sum^* \to \sum^*$ 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 $a,b\in\sum^*$，$f(a,b)$ 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 $a,b,c\in\sum^*$，存在 $f(f(a,b),c)=f(a,f(b,c))$。

4. 非交换律：对于任意的 $a,b\in\sum^*$，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。

5 新的基于 Merkle 树的移动代理路由解决方案

5.1 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）；

$h(.)$：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。

5.2 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，$i=0,1,\cdots,n$ 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

$\omega_0=y_0$

$\omega_i=f(\omega_{i-1},y_i)$，$i>0$

$z_0=f(u,x_0)$

然后计算

$U_i=E_{PK_i}(H_{i-1},H_i,H_{i+1},\omega_{i-1},t)$

$i=1,2,\cdots,n$

(2) 构造 2-3 元 Merkle 树

把叶结点置为 $(U_i,h(U_i))$ $i=1,2,\cdots,n$，代理主人按照 2-3元 Merkle 树的构造方式构造 2-3 元 Merkle 树。

(3) 签字

构造完 2-3 元 Merkle 树后，用户 H_0 对树的根结点 RV 进行签字 $S_0(RV)$。

(4) 移动代理的漫游

H_0 计算 $S_0(z_0,t)$，连同携带 Merkle 树的移动代理发送给主机 H_1。H_1 收到信息后，首先验证 H_0 的签名，得到 z_0。并且从 Merkle 树中抽取 U_1 的反向路径，重新计算从叶结点 $(U_1,h(U_1))$ 到根结点 RV 一路上的所有 hash 值，检查通过 U_1 和它的反向路径计算得到的根结点值 RV_1 是否与由 H_0 签名的 RV 相同。若一切合法，H_1 解密 U_1，获得 H_0，H_1，H_2 和 ω_0，得知代理后继主机是 H_2。然后，利用公开的 m,a_0,v，H_1 证实等式：$f(f(m,z_0),a_0)=f(v,\omega_0)$。否则，$H_1$ 直接将代理传回 H_0 并报告相应的错误信息。代理在 H_1 完成它的任务后，H_1 计算 $z_1=f(f(z_0,a_0),x_1))$，然后把 $S_1(z_1,t)$ 连同 Merkle 树剩余部分（将证实 $U_2,U_3,\cdots,U_n$ 反向路径所不需要的结点删除）传送给 H_2。

对于 $i=2,3,\cdots,n$，H_i 收到 H_{i-1} 传送过来的信息后，首先验证 H_{i-1} 的签名，得到 z_{i-1}。并且从剩余 Merkle 树中抽取 U_i 的反向路径，重新计算从叶结点 $(U_i,h(U_i))$ 到根结点 RV 一路上的所有 hash 值，检查通过 U_i 和它的反向路径计算得到的根结点值 RV_i 是否与由 H_0 签名的 RV 相同。若一切合法（否则，H_i 直接将代理传回 H_0 并报告相应的错误信息），H_i 解密 U_i，获得 H_{i-1}，H_i，H_{i+1}（$i=n$ 时为 H_{n-1}，H_n，H_0）和 ω_{i-1}，知道它的后继主机是 H_{n+1}（$i=n$ 时为 H_0），同时证实等式：$f(f(m,z_{i-1}),a_{i-1})=f(v,\omega_{i-1})$。

若一切合法（否则，H_i 直接将代理传回 H_0 并报告相应的错误信息），代理在 H_i 完成它的任务后，H_i 计算 $z_i=f(f(z_{i-1},a_{i-1}),x_i))$，把 $S_i(z_i,t)$ 连同 Merkle 树剩余部分（将证实 $U_{i+1},\cdots,U_n$ 反向路径时所不需要的结点删除）传送给 H_{i+1}。H_{i+1} 重复以上的过程，直到 H_n。最后，H_n 完成证实过程后，计算 $z_n=f(f(z_{n-1},a_{n-1}),x_n))$，把 $S_n(z_n,t)$ 连同移动代理传回 H_0。H_0 证实以下等式：$f(f(m,z_n),a_n)=f(v,\omega_n)$

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。

5.3 方案安全性分析

首先证明

$$f(f(m,z_i),a_i)=f(v,\omega_i),\ i=0,1,\cdots \tag{1}$$

证明：利用数学归纳法

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(1)成立，即

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

那么当 $i=k$ 时

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

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

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

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

下面针对安全性质 S1－S5 进行分析：

S1. 恶意主机若想修改路由信息，例如修改 U_i 为 $U_i'\neq U_i$。若要不被发现，则要求通过 U_i' 的反向路径计算所得的根结点值与通过 U_i 的反向路径计算所得的根结点值相同。由于选择的 hash 函数是单向、抗碰撞的，因此在计算上这是不可行的。

如果恶意主机 H_i 与 H_{j+1} 相勾结，企图删除 $H_{i+1}-H_j$ 的相关路由信息，但由于没有 $H_{i+1}-H_j$ 的帮助，恶意主机就无法得到 $z_{i+1},\cdots,z_{i+k-1}$，这样即便 H_{i+k} 是恶意的，由于没有 $z_{i+1},\cdots,z_{i+k-1}$，H_{i+k} 需要找到一组 $(\hat{\omega}_{i+k},\hat{z}_{i+k})$，使得等式 $f(f(m,\hat{z}_{i+k}),a_{i+k})=f(v,\hat{\omega}_{i+k})$ 成立。由于函数 f 的特性，我们知道 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，一旦发生路由信息恶意修改，就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。

S2. 用户 H_0 每次派发移动代理时，都要产生新的随机数 u，路由主机 H_i 每次都会计算新的 z_i。但是如果不知道 x_{i+1}，获得 z_i 对于 z_{i+1} 的计算没有任何意义。所以，主机 H_i，$i=1,2,\cdots$ 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。

S3. 由协议可以看到，主机 H_i，$i=1,2,\cdots$ 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。

S4. 主机间所具有的 IP 协议可以使该性质得到满足。

S5. 路由信息中的时戳 t 可以证实是否发生重放攻击。

5.4 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，如表 1 所列。

表 1 不同方案比较

计算复杂度及信息传输量 / 路由方案	用户		路由主机	
	加密	签字	加密	签字
文献[4]	n(n+1)/2	n(n+1)/2	n(n+1)/2	n(n+1)/2
文献[5]	n(n+1)/2	n	n	n(n+1)/2
文献[6]	n	2	3n	3n
本文方案	n	2	2n	2n

1. 用户方面：H_0 构造好 Merkle 树后，需要对根节点进行一次签名。另外要对 z_0 进行一次额外签名，对路由信息进行 n 次加密。

2. 路由主机方面：从方案处理过程可以看出，每一路由主机 $H_i(i=1,2,\cdots,n)$ 只需验证两次签名，进行一次解密和一次签名操作。因此，路由主机总的计算复杂度为：签名(解密)为 $2n$，加密(验证签名)为 $2n$。

结束语 移动代理的安全问题一直是困扰其广泛应用的一个绊脚石。本文利用一种特殊单向函数，结合 Merkle 树结构，从新的角度构造了一个基于 Merkle 树的移动代理路由解决方案。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[6]，从而简化了用户的工作，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，姜正涛，王育民. 基于 Merkle 树的安全移动代理路由协议及其推广[J]. 电子学报，2005，33(7)：1250-1253

[7] Hemaspaandra L A, Rothe J, Saxena A. Enforcing and Defying Associativity, Commutativity, Totality, and Strong Noninvertibility for One-Way Functions in Complexity Theory[R]. URCSD; 854. University of Rochester, December 2004