第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)07—0154—03 文献标识码：A 中图分类号：TP393

可证明安全的移动代理路由协议

田 旭[1]，刘仁金[2]，陈明华[2]
(1. 皖西学院现代教育技术中心，六安 237012；2. 皖西学院计算机科学与技术系，六安 237012)

摘 要：针对移动代理路由安全问题，利用 Hash 函数单向性和迭代方法提出一种移动代理路由协议。用户主机通过 Hash 函数的单向性保证路由信息安全到达路由主机，路由主机之间根据 Hash 函数值的迭代进行交互认证。该协议的计算复杂度显著降低，特别是在大数据传输的情况下。采用常规方法和串空间模型方法分析并证明了该协议的安全性。

关键词：移动代理；迭代；单向散列；串空间；计算复杂度

Provable Security Mobile Agent Routing Protocol

TIAN Xu[1], LIU Ren-jin[2], CHEN Ming-hua[2]
(1. Modem Education Technological Center, West Anhui University, Lu'an 237012;
2. Department of Computer Science & Technology, West Anhui University, Lu'an 237012)

【Abstract】 A new mobile routing protocol using Hash function and iterative method is proposed in this paper for solving mobile agent routing security problems. User hosts are able to ensure routing information transporting to the others securely by the unidirectional feature of Hash function, and verify each other by the iteration of Hash function. The analysis shows that the computational complexity of the routing protocol is drastically reduced, especially in the condition of transporting large number of data. The normal and the strand space models are adopted to prove the security of the protocol.

【Key words】 mobile agent; iterative; Hash function; strand space; computational complexity

1 概述

移动代理是替代用户和其他程序执行设定任务的程序，在网络中按源主机的设定，自主地在主机之间迁移。作为一种新型的分布式计算模型，移动代理已经在移动计算、智能网以及电子商务等领域得到广泛应用。但移动代理的安全问题使其在实际应用中面临困境，路由安全问题是其中的关键问题之一。

针对移动代理路由的安全问题，文献[1-4]分别给出了解决方案。其中，文献[3-4]的方案具有较好的安全性，文献[4]的解决方案最优。但已有方案均存在需要进行多次加解密操作和大数据加密问题，这对资源要求苛刻的网络设备而言，有一定的局限性。鉴于以上情况，本文利用 Hash 函数的不可逆性质和迭代方法，提出了一种新的移动代理路由协议。用户主机通过减少签名的信息量，避免对大数据的非对称密钥签名操作；在路由信息认证阶段，路由主机无须采用非对称密钥加密签名认证，减少了加解密的次数。经分析，本协议能显著降低用户主机和路由主机的计算复杂度。

2 已有移动代理路由协议分析

2.1 协议表示符号

已有协议[1-4]的符号设定如下：

(1)H_0：源主机IP地址；

(2)H_i：路由主机IP地址，i=1,2,…,n；

(3)PK_i：主机H_i的公开密钥；

(4)SK_i：主机H_i的私钥；

(5)ENC_i()：用公开密钥SK_i加密；

(6)Sig_i()：用私有密钥PK_i签名；

(7)||：连接符号；

(8)⊕：异或运算；

(9)$Code_i$：移动代理在路由主机H_i上的执行程序代码；

(10)*Hash* ()：安全的单向散列函数；

(11)*HMAC*()：钥控单向散列函数；

(12)T：时间戳。

2.2 常规协议的计算复杂度分析

已有路由协议[5]的计算复杂度见表 1。

表 1 已有路由协议计算复杂度比较

路由方案	用户主机		路由主机	
	加密(验证签字)	签字(解密)	加密(验证签字)	签字(解密)
文献[1]	$n(n+1)/2$	$n(n+1)/2$	$n(n+1)/2$	$n(n+1)/2$
文献[3]	$n(n+1)/2$	n	n	$n(n+1)/2$
文献[5]	$n+1$	$n+1$	$3n$	$3n$

从表 1 中得出，文献[4]的路由主机每次进行路由移动时须 6 次非对称密钥加密解密操作，用户主机需要 $2n+2$ 次。而非对称密钥加解密操作耗费大量计算资源；且随着技术的进步，需要更高强度的密钥才能保证数据安全，这意味着密钥长度的加长，需要更多的计算资源。另一方面，已有安全移动代理路由协议都需要对大数据进行加解密操作(主要是移动代码内容的长度)。在非对称密钥(如文献[4]中设定 RSA 密钥长度为 1 024 b)加密体系中，明文块的长度应小于加密密钥长度，密文长度等于解密密钥长度。对大数据加密，须先

基金项目：安徽省教育厅自然科学基金资助项目(2006KJ046B)
作者简介：田 旭(1972－)，男，讲师，主研方向：计算机网络；刘仁金，博士、副教授；陈明华，教授
收稿日期：2007-05-10 **E-mail：**tianxu27@126.com

对大数据分解，再分别对小数据加密。而移动代码的内容长度会轻易超过加密密钥长度。因此，已有移动代理路由协议的计算复杂度远超出表 1 的分析。

3 一种新的移动代理路由协议

本文针对以上计算复杂度和大数据加密方面的缺陷，根据Hash函数的单向性，提出了一种新的移动代理路由协议。尽管常用单向散列函数如MD5, SHA已被破解，但目前还是相对安全的。因此，本文采用迭代和异或运算结合的方法加强其安全性。以*Routeri*表示路由信息，HC_i 表示请求验证消息，HS_i表示确认信息，协议具体如下：

(1)初始化

鉴于常用 Hash 函数已不能保证绝对安全，同时为了防止多台不诚实路由主机相互勾结、提前泄露秘密，这里采用了双散列认证和异或运算结合的方式，既保证了认证口令的安全性，又防止了不诚实路由主机跳过某些路由主机。

Step1 用户主机H_0选择一段数据S，所选数据应满足一定的长度要求。采用指定的散列算法(如MD5, SHA)将S经若干次散列生成一系列口令。第 1 台路由主机使用的口令是S的$2n+1$次(n为路由主机数量)散列值，即

$$Hash^{2n+1}(S)=Hash(Hash(Hash^{2n-1}(S)))$$

第 2 台主机的口令为

$$Hash^{2n-1}(S)=Hash(Hash(Hash^{2n-3}(S)))$$

…

第 n 台主机的口令为 $Hash(S)$。

由于散列函数具有不可逆性，这样攻击者即使能监视口令的传输也不能伪造下一次口令。

Step2 用户主机H_0产生随机数$R_0, R_2,\cdots, R_n$，保存

$$Hash^{2n+1}(S),\ R_0,\ Hash(S),\ Hash(R_{n-1}),\ R_n$$

以对路由主机进行认证。

(2)用户主机H_0计算路由信息

$M_i=[H_{i-1}, H_i, H_{i+1}, H_0, Code_i]$

$Router1=[Hash^{2n+1}(S) \oplus Hash^3(R_0)]||$

…

If M_i 长度>密钥长度

$ENC_i(M_i,\ Sig_0(Hash^{2n-2i+3}(S) \oplus Hash^{2n-2i+1}(S),\ Hash(R_{i-1}),\ R_i,\ T,\ Hash(M_i)))$

Else

$ENC_i(H_0,\ Sig_0(M_i, Hash^{2n-2i+3}(S) \oplus Hash^{2n-2i+1}(S),\ Hash(R_{i-1}),\ R_i,\ T))$

…

(3)移动代理漫游过程

Step1 H_0计算路由*Router*1 后，将移动代理发出。

Step2 H_1收到路由消息后，用私钥对第 2 部分解密。根据$Hash(R_0)$ 计算出$Hash^3(R_0)$，按照异或运算的性质，对第 1 部分进行一次异或运算即可计算出$Hash^{2n+1}(S)$。这样既可验证$Hash^{2n-1}(S)$的值，又可计算出$Hash^{2n-1}(S)$作为下一个路由主机的确认口令。

Step3 H_1计算

$$Hash^{2n}(S)=Hash(Hash^{2n-1}(S))$$

将

$$HC_1=[Hash^{2n}(S) \oplus Hash^2(R_0)]$$

发送到H_0；用户主机根据R_0的值计算$Hash^2(R_0)$，再对HC_1的值进行一次异或运算，得出$Hash^{2n}(S)$的值：

$$Hash^{2n+1}(S)=Hash(Hash^{2n}(S))$$

由此可以验证H_1。

Step4 H_0计算

$$HS_1=[HMAC(Hash^{2n}(S)||PK_0||Hash(R_0)||PK_1||t,\ PK_0),\ t]$$

并发送给H_1，H_1检验HS_1，时间戳可以保证签名的新鲜性。HS_1包含H_1的公钥，可以保证HS_1是H_0 发送给H_1 的，且不必担心泄露路由信息。

Step5 H_1根据路由向下一站路由主机H_2发送代理：

$Router2=[Hash^{2n-1}(S) \oplus Hash^3(R_1)]||$

$ENC_2(\cdots)||$

…

$ENC_n(\cdots)$

执行*Step*2~*Step*5，直到路由主机H_n收到消息：

$Routern=[Hash^3(S) \oplus Hash^3(R_{n-1})]||ENC_n\ (H_0,\ H_{n-1},\ H_n,\ H_0,\ Hash^3(S) \oplus Hash(S),\ Hash(R_{n-1}),\ R_n,\ T,\ Code_n)]$

H_n经计算将

$$[HMAC(Hash^2(S)||(Hash(R_{n-1})||R_n||t,\ PK_n),\ t)$$

发送给用户主机，用户主机可验证移动代理是否经过了所有指定的诚实主机。

漫游过程如图 1 所示。

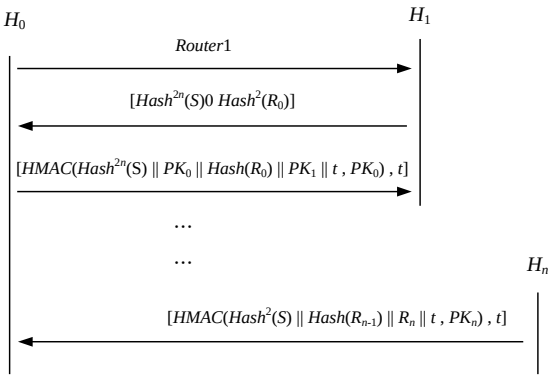

图 1 移动代理路由漫游示意图

4 新协议计算复杂度分析

(1)用户主机

用户主机H_0计算路由*R*outer1 时需要进行n次签名、n次加密，还须计算 $3n+1$ 次*Hash*值，与H_1进行认证须进行 2 次异或运算和 4 次散列值计算。由于散列函数和异或运算的计算量非常小，可以忽略不计，因此用户主机总计算复杂度为 $2n$，如表 2 所示。

表 2 一般情况下各路由协议计算复杂度比较

路由方案	用户主机		路由主机	
	加密(验证签字)	签字(解密)	加密(验证签字)	签字(解密)
文献[1]	$n(n+1)/2$	$n(n+1)/2$	$n(n+1)/2$	$n(n+1)/2$
文献[3]	$n(n+1)/2$	n	n	$n(n+1)/2$
文献[4]	$n+1$	$n+1$	$3n$	$3n$
本文方案	n	n	n	n

(2)路由主机

经分析，本协议中每一路由主机只须进行 4 次异或运算、6 次散列运算，与主机在路由中的位置无关。路由主机总计算复杂度为 $2n$，如表 2 所示。

(3)大数据加密

新协议与已有协议相比，需要签名的数据长度很短(3 个*Hash* 值、1 个随机数 *R*、时间戳 *t*、长度远小于加密密钥长度)，如果将发送给每个路由主机的明文数据均分成 $k(k \geq 2)$份，常规方案至少须进行加密和签名 $2k$ 次；本方案仅需要 $k+1$ 次。如表 3 所示。

表 3　传输大数据情况下各路由协议计算复杂度比较($k \geq 2$)

路由方案	用户主机		路由主机	
	加密(验证签字)	签字(解密)	加密(验证签字)	签字(解密)
文献[1]	$n(n+1)k/2$	$n(n+1)k/2$	$n(n+1)k/2$	$n(n+1)k/2$
文献[3]	$n(n+1)k/2$	kn	kn	$n(n+1)k/2$
文献[4]	$kn+1$	$kn+1$	$kn+2n$	$kn+2n$
本文方案	$kn+n$	n	n	$kn+n$

5　安全性分析

5.1　常归分析

(1)如果某个主机企图使移动代理跳过诚实主机H_i直接到达H_{i+1}，则需要计算出

$Hash^{2n-2i+1}(S) \oplus Hash^3(R_i)$

否则，主机H_{i+1}可立即发现异常。如果H_{i+1}是诚实的，立即向用户H_0报告；同时主机H_{i+1}计算不出到达下一站的确认口令，后继主机也不能确认代理的来源。因此，本协议可以保护移动代理经过所有的诚实主机，并且一旦路由信息遭恶意修改，可以很快地被距离恶意主机最近的诚实主机发现。

(2)假设路由主机没有泄露私钥，除了知道本机的前驱和后继主机外，不能获取更多的路由信息；而对于代理路由外的主机，由于没有任何路由主机的私钥，因此不能获得任何路由信息。

(3)路由主机通过用户主机的签名信息，确认自己是代理的一部分。

(4)通过用户主机的签名和 Hash 函数的单向性，路由主机能确认路由信息来自前驱主机。

(5)通过用户主机的签名和时间戳，证实是否发生重放攻击。

由于 Hash 函数的单向性，攻击者根据已有信息 $Hash(x)$，无法计算原像 x；且本文提出的协议是经过多次散列得出，破解难度更大。虽然异或运算的不可逆性不能很好地保证协议的安全性，但 Hash 函数的长度(例如 MD5 为 128 位，SHA-1 为 160 位)足够保证攻击者不能通过穷举法进行破解。异或运算和 Hash 函数的结合能完全保证协议的安全。

5.2　串空间模型分析

本文采用串空间模型对改进路由协议进行分析。认证测试规则是应用于协议分析的方法，共有 3 种重要的认证测试[5]方法：出测试，入测试和主动测试。测试规则的使用能够简化协议分析的过程。

改进路由协议的串空间构造如下：

(1)发起者串

$Initi[H_{i-2}, H_{i-1}, H_i, PK_{i-1}, PK_i, Hash^{2n-2i+1}(S), Hash^{2n-2i}(S), R_{i-1}, Hash(R_{i-2}), t] = <+Routeri, -HC_i, +HS_i>$

(2)响应者串

$Respi[H_{i-1}, H_i, H_{i+1}, PK_{i-1}, PK_i, Hash^{2n-2i-1}(S), Hash^{2n-2i-3}(S), R_i, Hash(R_{i-1}), t] = <-Routeri, +HC_i, -HS_i>$

(3)前提假设

$SK_i \notin Kp(i=1, 2, \cdots, n)$, $R_1 \neq R_2 \neq \cdots R_{n-1} \neq R_n$

串空间如图 2 所示。

(1)响应者对发起者的认证

前提假设：令C为Σ中的簇，S为响应者串，$SK_i \notin Kp$。

证明：

1)构造测试分量。

响应者串为

$H_i = ENC_i(M_i, Sig_i(Hash^{zn-2i+3}(S \oplus Hash^{2n-2i+1}(S), Hash(R_{i-1}), R_i, T, Hash(M_i)))$

由于$Hash(R_{i-1})$唯一产生于$<H_i, 2>$，由图 2 可以得出，$<H_i, 2> \Rightarrow {}^+< H_i, 3>$是$R_{i-1}$的出测试。

2)应用认证测试规则 1，得到存在正常节点 $N, N' \in C$，

$term(N) = (Hash^{2n-2i+2}(S) \oplus Hash^2(R_{i-1}))$

并且$N \Rightarrow {}^+N'$是R_{i-1}的转换边。

3)由第 2)步的结果可得，节点N为负节点，这时N只能是$<H_{i-1}, 2>$，其中，

$H_{i-1} \in [H_{i-2}, H_{i-1}, H_i, R_i, PK_{i-1}, PK_i, Hash^{2n-2i+1}(S), Hash^{2n-2i}(S), R_{i-1}, Hash(R_{i-1}), t]$

于是，变换边$N \Rightarrow {}^+N'$必为$<H_i, 2> \Rightarrow <H_{i-1}, 3>$，且

$C\text{-}hight(H_i) = 3$

因此，响应者成功地证明了发起者。

(2)发起者对响应者的认证

同理可以证明。

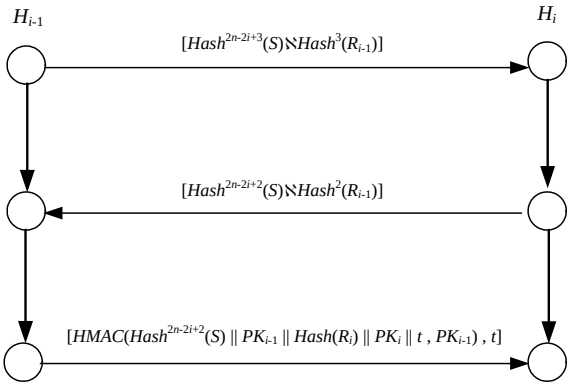

图 2　改进路由协议的串空间

6　结束语

移动代理由于其自身所具有的优异特性，已经在很多领域得到了应用，但安全问题一直是妨碍其发展的主要原因之一。本文指出了已有移动代理路由协议存在的计算复杂度大和大数据加密问题，提出了一种基于散列函数和多重迭代方法的改进代理路由协议，显著降低了其计算复杂度。本文用常规和串空间 2 种方法分析并证明了本路由协议的安全性。

参考文献

[1] Domingo J. Mobile Agent Route Protection Through Hash-based Mechanisms[C]//Proc. of INDO-CRYPT'01. Berlin: Springer-Verlag, 2001.

[2] Sander T, Tsehudin C F. Protecting Mobile Agents Against Malicious Hosts[C]//Proc. of Conference on Mobile Agents and Security. Berlin, Germany: Springer-Verlag, 1998.

[3] Mir J, Borrell J. Protecting General Flexible Itineraries of Mobile Agents[C]//Proc. of ICICS'01. Berlin, Germany: Springer-Verlag, 2002.

[4] 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): 50-54.

[5] Guttman J D, Fabrega F J T. Authentication Tests and the Structure of Bundles[J]. Theoretical Computer Science, 2002, 283(2): 333-380.