移动IPv6网络安全接入认证方案

张 志[1,2] 崔国华[1]
(华中科技大学计算机科学与技术学院 武汉 430074)[1]
(武汉职业技术学院计算机技术与软件工程学院 武汉 430074)[2]

摘 要 对于移动IPv6网络,身份认证是网络安全的关键问题之一。针对移动IPv6网络的接入认证,提出了一种基于移动互联网双向认证方案。在移动切换过程中的接入认证和家乡注册,采用对家乡注册消息进行基于双私钥签名的方式,实现了家乡代理和移动节点分别对注册消息的签名,实现了接入认证与家乡注册的并发执行,移动用户和接入网络的一次交互实现了用户和接入域的有效双向认证。理论分析和数据结果表明,方案的认证总延时和切换延时要优于传统方法,有效地降低了系统认证的延时。安全性分析表明,框架中的基于双私钥的CPK方案满足双向接入认证安全,有效地解决了密钥托管问题。

关键词 移动IPv6,接入认证,切换性能,组合公钥,基于身份签名
中图法分类号 TP309 **文献标识码** A

Secure Access Authentication Scheme in Mobile IPv6 Networks

ZHANG Zhi[1,2] CUI Guo-hua[1]
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(College of Computer Technology and Software Engineering, Wuhan Institute University, Wuhan 430074, China)[2]

Abstract To Mobile IPv6 networks, identify authentication is crucial issues of the network security. This paper proposed a secure identify authentication scheme, which considers inters domain reputation relationship between mobile node home domain and the access domain in the pre-handoff procedure and realizes effective mutual authentication between mobile node(MN) and the access domain. Authentication can be accomplished by double private key, HA and MN signing the home registration messages respectively. The access authentication can be accomplished in the visited network instead of the home network, and the handover procedure integrating authentication only needs one round trip. Theoretical analysis and numerical results show that proposed scheme is more effective in reducing total authentication and handoff delay and the signaling overhead than relative schemes. Based on the security of CPK algorithm and IBS, we prove the access authentication and home registration process handover latency of ours is better than that of the existing solutions and our solution satisfies mutual authentication security, resolves the key escrow efficiently.

Keywords Mobile IPv6, Access authentication, Handover performance, Combined public-key, Identity-based signature

1 引言

随着IP技术和无线通信技术的发展和融合,用户对移动网络的需求日益增强,无线移动网络已经成为下一代互联网络的发展方向。为了能够提供安全有效的移动IPv6服务,当移动用户从外地域接入网络时,需要家乡域和接入域协作实现对移动用户的身份认证,例如可采用AAA(Authentication, Authorization, And accounting)[1]等技术实现。目前,在AAA架构[1,2]中的移动IPv6依靠经常查询的家乡网络来验证移动节点的身份,不可避免地会增加切换延时。为了解决这个问题,国内外学者展开了热烈的探讨。基于消息捎带的策略[3],在认证消息中捎带移动注册消息以减小处理延时;基于二层"暗示"的策略[1],利用二层触发信号,在移动节点(Mobile Node, MN)移动到新子网前,就开始认证和预切换处理;基于上下文转移的策略[2],通过认证信息在各认证实体间的上下文转移,减少切换过程中由认证带来的附加开销;基于移动IP增强协议的策略[1,4],将接入认证与移动IP的增强方案结合以提高认证切换性能。上述策略都是从某一个角度去研究如何将接入认证过程更好地加入到现有的各种移动解决方案中,并没有将移动切换过程和接入认证过程进行更有机的融合,也没有考虑减少接入认证过程后给切换延时带来的影响。文献[5]提出了一种基于身份的密钥方案,通过IBS算法,解决了上述基于证书的认证方法存在的问题,但没有考虑引入认证过程后对切换性能带来的问题,而且也没能解决密钥托管问题。文献[6]提出基于身份签名的层次化认证方法,采用两层身份签名技术AAAv与AAAh一次交互完成MN

到稿日期:2009-01-20 返修日期:2009-03-30 本文受国家自然科学基金项目(60703048),湖北省自然科学基金项目(2007ABA313)资助。
张 志(1977-),女,博士研究生,主要研究方向为网络安全、密码学等,E-mail:amiee_zhang@163.com;崔国华(1947-),男,教授,博士生导师,主要研究方向为访问控制、密码体制的安全性分析、代数数论。

与接入网络的双向认证，但这只能部分解决密钥托管问题。

受 Katz-Wang[7] 的双公钥思想的启发，本文设计了一种基于组合公钥(Combined Public-Key，CPK)体制[8]和双私钥的签名方案，以有效地解决密钥托管问题。并在此基础上提出了一种适用于移动 IPv6 网络环境的并行接入认证机制。该机制利用基于 CPK 和双私钥签名方案的特性，将移动切换过程和认证过程进行有机整合，采用基于 CPK 身份签名技术，并发实现接入认证和位置登记阶段的家乡注册，认证总延时和切换延时要优于传统方法，有效地降低了系统认证的延时，提高了整体性能。同时，在随机预言机模型下证明了方案的安全性。本文第 2 节介绍基于身份的短签名和 CPK 算法；第 3 节详细描述基于 CPK 的安全认证方法；第 4 节对该切换方法进行性能分析和安全性分析；最后对本文进行总结。

2 预备知识

2.1 基于身份的短签名方案

基于身份的短签名方案[9]由系统参数的建立、密钥生成、签名和验证 4 个阶段构成，具体描述如下。

Setup：输入系统安全参数 k，选取两个大素数 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2、双线性映射 $\hat{e}:G_1\times G_1\to G_2$，$G_1$ 的生成元 P，强杂凑函数 $h:\{0,1\}\times G_2\to Z_q^*$。

Extract：给定用户 $ID\in\{0,1\}^*$，用户执行如下步骤。

1)随机选取私钥 $x\in Z_q^*$；

2)计算 $R=xP$，则 (P,R) 就是用户的公钥。

Sign：1)计算 $\sigma=x\cdot H(M)$；

2)发送签名就是 (M,σ) 给验证者。

Verify：验证者收到签名后，可通过如下等式验证签名：$\hat{e}(M,\sigma)=\hat{e}(H(M),R)$，若等式成立，则签名正确。

2.2 CPK 算法

组合公钥(combined public key，CPK)[8]算法是基于椭圆曲线密码系统构建的，理论依据是离散对数问题的难解性，CPK 算法如下：

选择有限域 $Ep(p\neq2,p\neq3)$ 上的椭圆曲线 $y^2\equiv x^3+ax+b \bmod p$ 的所有解 $p=(x,y)$ 加上一个无穷远点 $\odot$ 点构成椭圆曲线群，记为 $E(a,b)$。椭圆曲线密码技术的加、解密主要是利用椭圆曲线上的点的标量乘来实现的。假定椭圆曲线密码系统的参数为 $T=(a,b,G,n,p)$，其中 a,b 为椭圆曲线参数，G 为椭圆曲线上的基点，n 为椭圆曲线上点的阶，p 为素数域 F_p 的阶。如果假定用户的私钥为素数域 F_p 上的任一整数 $SK=r$，那么对应的公钥 PK 即为椭圆曲线 E 上的点 $r\cdot G$。将一定数量的公、私钥因子对分别组成公钥因子矩阵和私钥因子矩阵 $m\times n$(m 行 n 列)。私钥因子矩阵 SSK 中的元素即为整数标量 r_{ij} $(1\leqslant i\leqslant m)$，而公钥因子矩阵中的元素即为与私钥因子 r_{ij} 对应的椭圆曲线上的点 $r_{ij}\cdot G$。在密钥管理中心生成公、私钥因子矩阵后，私钥因子矩阵需要保持秘密，而公钥因子矩阵则予以公布。

私钥因子矩阵

$$SK=\begin{Bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ r_{11} & r_{12} & \cdots & r_{1n} \end{Bmatrix},$$

公钥因子矩阵

$$PK=\begin{Bmatrix} r_{11}G & r_{12}G & \cdots & r_{1n}G \\ r_{21}G & r_{22}G & \cdots & r_{2n}G \\ \cdots & \cdots & \cdots & \cdots \\ r_{11}G & r_{12}G & \cdots & r_{1n}G \end{Bmatrix}$$

CPK 具有简便、易行、经济和高效等优越的特性，并且具有分割性、CPK 信任性的传统密钥管理优点。现在，本文将其用作公开公钥生成方法，并分析说明协议的可行性。

3 层次化认证方法

本节提出的层次化认证方法采用两层身份签名机制实现双向认证功能。首先分析了该方法的设计思想，然后详细介绍了该方法的实现原理。

3.1 基于 CPK 双私钥签名和验证方案

结合 CPK 体制 IBS 签名和验证方案包括参数建立、签名及验证等阶段[8]。

Setup：输入系统安全参数 k，密钥管理中心进行如下初始化过程。

1)选取两个大素数 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2、双线性映射 $\hat{e}:G_1\times G_1\to G_2$，$G_1$ 的生成元 P，强杂凑函数 $h:\{0,1\}\times G_2\to Z_q^*$。

2)生成 2 个 $l\times h$ 阶私钥种子矩阵 $PriKSM$：

$\begin{pmatrix} r_{1,1}^0 & \cdots & r_{1,h}^0 \\ \vdots & \ddots & \vdots \\ r_{l,1}^0 & \cdots & r_{l,h}^0 \end{pmatrix}$ 和 $\begin{pmatrix} r_{1,1}^1 & \cdots & r_{1,h}^1 \\ \vdots & \ddots & \vdots \\ r_{l,1}^1 & \cdots & r_{l,h}^1 \end{pmatrix}$，其中 $r_{i,j}^0$ 和 $r_{i,j}^1$ 在 Z_q^* 内随机选取。

生成相应的 2 个 $l\times h$ 公钥种子矩阵 $PubKSM$：阶

$$PubKSM:\begin{pmatrix} r_{1,1}^0P_0+r_{1,1}^1P_1 & \cdots & r_{1,h}^0P_0+r_{1,h}^1P_1 \\ \vdots & \ddots & \vdots \\ r_{l,1}^0P_0+r_{l,1}^1P_0 & \cdots & r_{l,h}^0P_0+r_{l,h}^1P_1 \end{pmatrix}$$

3)选取两个函数集 $F_0=\{f_1,f_2,\cdots,f_h\}$ 和 $F_0=\{f_1,f_2,\cdots,f_h\}$，每个函数集包含 h 个不同的伪随机函数，且满足对 $\forall i\in[1,h]$ 和 $ID\in\{0,1\}^*$ 有 $index_i\in[1,m]$，其中 $index_i=f_i(ID)$。

4)保密私钥种子矩阵 $PriKSM$ 和主密钥 s，公开系统参数 $params=\langle q,G_1,G_2,\hat{e},P,g_1,g_2,F,PubKSM\rangle$。

Extract：给定用户 $ID\in\{0,1\}^*$，令用户的公私钥分别为 PK_{ID} 和 SK_{ID}，令 $index_1=f_1(ID),\cdots,index_h=f_h(ID)$，密钥管理中心随机选取 $s_1\in Z_q^*$ 则公钥 $PK_{ID}=((r_{index_1,1}^0P_0+r_{index_1,1}^1P_1)+\cdots+(r_{index_h,h}^0P+r_{index_h,h}^1P))\in G_1^*$，则双私钥分别为 $SK_{ID}^0=(r_{index_1,1}^0+\cdots+r_{index_h,h}^0) \bmod q\in Z_q^*$，$SK_{ID}^1=(r_{index_1,1}^1+\cdots+r_{index_h,h}^1) \bmod q\in Z_q^*$，$r_{index_i,i}^0$ 和 $r_{index_i,i}^1$ 分别是矩阵 $PriKSM_0$ 和 $PriKSM_1$ 中的元素，所以即有 $PK_{ID}=SK_{ID}^0\cdot P_0+SK_{ID}^1\cdot P_0$。私钥为 $SK_{ID}=\langle SK_{ID}^0,SK_{ID}^1\rangle$，这就形成了公私钥对。将私钥 SK_{ID}^0 和 SK_{ID}^1 分别发送给家乡代理和移动节点。

Sign：签名分为家乡代理签名和移动节点签名两个部分。

移动节点签名：对于给定的消息 m，签名过程如下。

1)计算 $\sigma_0=\langle P,H_1(M)\cdot SK_{ID}^0\rangle$；

2)将签名 $\sigma_0\in G_1\times Z_q^*$ 发送给验证者。

HA 签名：家乡代理对于给定的消息 m，签名过程如下：

1)计算 $\sigma_1=\langle R,H_1(M)\cdot SK_{ID}^1\rangle$；

2)将签名 $\sigma_1\in G_1\times Z_q^*$ 发送给验证者。

Verify：验证者收到 σ_0 和 σ_1 两部分签名，计算：

1)运行 Extract 算法获得用户公钥 PK_{ID}；

2)计算 $v=\sigma_0\times\sigma_1$，判定等式：

$$v=\sigma_0\times\sigma_1=\hat{e}(P,H_1(M)\cdot SK_{ID}^0)\hat{e}(P,H_1(M)\cdot SK_{ID}^1)$$
$$=\hat{e}(P,H_1(M)\cdot SK_{ID})$$
$$=\hat{e}(PK_{ID},H_1(M))$$

验证是否成立。若成立，则输出 T；否则输出 F。

3.2 层次化认证方法的基本思想

在 MIPv6 网络中，当 MN 发生移动时，移动 MN 和接入域需要进行双向认证。对于合适的 MN，由于其认证存放在家乡网络，必须通过与家乡网络认证服务器的交互来实现移动节点认证，因而认证延时和开销将随着访问网络与家乡网络之间距离的增加而显著增大。为了解决这个问题，人们提出层次化位置登记策略[10]。引入 MAP，网络由第一层(PKGMaps 和 HA)、若干第二层用户(ARs 和 MN 等)组成。每一个 MAP 管理着若干访问路由器。MN 在同一个 MAP 域移动时，只需执行本地注册。MN 接入新访问域后，在完成绑定更新时只需与接入的 AR 利用对发送消息的签名来完成双向认证过程。

本方案采用结合 CPK 和双私钥的 IBS 方案可以实现：1)签名的验证功能仅取决于签名参数，任何节点均可很容易地获取。利用该特点，就可实现 MN 直接与接入网络的认证服务器交互以完成接入认证，从而消除两个认证服务器之间的通信延时开销。2)采用双私钥的签名方案中，MN 不知道 HA 的私钥，HA 也不知道 MN 的私钥，为了签名，MN 必须首先从 HA 那里获得指定消息的部分签名信令，没有这个信令 MN 不能使用其部分私钥来签名消息。家乡网络的认证利用上述优势，就可实现 MN 直接与接入网络的认证服务器交互以完成接入认证，从而消除两个认证服务器之间的通信延时开销。同时，相对于其他公钥签名机制(如公钥证书机制)，IBS 机制简化了公钥的获取，消除了对公钥证书和认证中心的依赖，从而消除了 MN 因为获取公钥证书和维护公钥证书产生的额外开销。

在移动 IPv6 中，MN 每次移动都要执行绑定更新，如果 MN 远离家乡，将会带来很大的延时和开销。它的基本思想是：采用层次化移动管理，层次化移动 IPv6 协议便能有效减少因发送大量注册消息带来的延时、信令开销以及带宽开销。具体实现如图 1 所示。

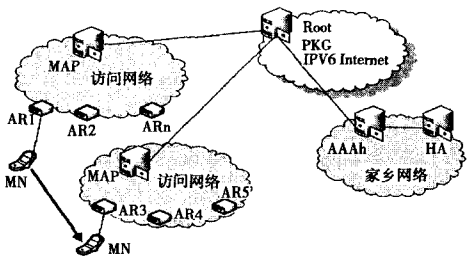

图 1 层次化快速认证系统框架

3.3 层次化认证方法的实现

层次化认证方法包括预切换和接入认证两个阶段，具体流程如图 2 所示。预切换过程详细描述如下：

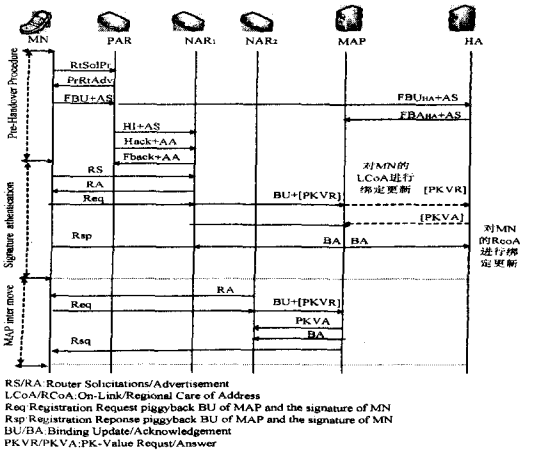

图 2 层次化认证方法实现流程

1) $HA\rightarrow MN:\langle BA_{HA}||TS||\{BU_{HA}||R_{MN}||\mathrm{RrVa}\}Sign_{HA}\rangle$

MN 准备移入新的子网时，数据链路层若检测到信号强度的变化，则触发快速切换过程的开始。MN 请求 HA 对 BU_{HA} 进行半签名。

2) $HA\rightarrow MAP:\langle BA_{HA}||TS||\{BU_{HA}||R_{MN}||\mathrm{RrVa}\}Sign_{HA}\rangle$

HA 检查：MN 若没有被撤销，则生成 MN 家乡注册的绑定更新确认消息 BU，并使用自己掌握 MN 的半私钥对该消息进行半签名，完成 HA 对 MN 的认证并将认证消息发送给 MAP。否则，返回错误消息给 MN。

3) $MN\rightarrow NAR:\mathrm{Re}\ q=\langle BU_{HA}||TS||\{BU_{HA}||TS\}Sign_{MN}||PK_{MN}||ID_{MN}\rangle$

当 MN 移动到新的子网，根据收到 NAR 发送的路由器宣告消息，生成子网前缀 LCoA 和 RCoA，利用根 PKG 生成公开参数 $params$，MN 根据签名机制中的 Sign 算法对绑定更新消息计算自己的半签名，然后根据其保存的 HA 的半签名计算 $\{BU_{HA}||TS\}Sign_{MN+HA}$，并将绑定更新消息连同签名和身份组成 Req 消息发送给 NAR。

4) $NAR\rightarrow MAP:\langle BU_{MAP},BU_{HA},[PKVR]\rangle$

NAR 收到 AReq 消息后，取出 $\langle BU_{MAP},BU_{HA},[PKVR]\rangle$ 消息并发送给 MAP。然后 MN 的身份 ID，运行 Extract 算法获得用户公钥 PK_{ID}，验证签名 $\{BU_{HA}||TS\}Sign_{MN+HA}$，同时检查时间戳 TS_1，保证签名消息的新鲜性。当验证成功后，完成接入网络对 MN 的认证。为了提高效率，NAR 先发送 $\langle BU_{MAP},BU_{HA},[PKVR]\rangle$ 消息，查询用户公钥 PK_{ID}，然后验证签名，从而实现绑定更新与验证的并发执行。

5) $MAP\rightarrow NAR:\langle\{BA_{MAP}\}ID_{MAP}\rangle$

MAP 验证了 MN 的签名并确信绑定更新消息为经过 HA 和 MN 双私钥签名后，则完成对 MN 的 LCoA 的位置登记，并用公开的用户身份 ID_{MAP} 对 BA_{MAP} 进行签名。

6) $NAR\rightarrow MN:ARsp=\langle BA_{MAP}||TS_1||TS_2||\{BA_{MAP}||TS_1\}Sign_{MAP}||\{BA_{MAP}||TS_2\}Sign_{NAR}\rangle$

①NAR 收到 MAP 发送来 $\langle BA_{MAP}||TS_1||TS_2||\{BA_{MAP}||TS_1\}Sign_{MAP}\rangle$ 消息后，取出其中的绑定确认消息，使用自己的私钥对绑定确认消息进行签名 $\{BA_{MAP}||TS_2\}Sign_{NAR}$，然后将绑定确认消息连同签名和收到的 MAP 的签

名组成 Rsp 消息并发送给 MN。

②MN 收到 Rsp 消息后，取出其中的绑定确认消息，完成位置登记过程；MN 取出 ARsp 中的签名，首先验证 MAP 的签名$\{BA_{MAP}||TS_1\}Sign_{MAP}$，同时检查时间戳$TS_1$，保证签名消息的新鲜性；然后验证 AR1 的签名$\{BA_{MAP}||TS_2\}Sign_{NAR}$，同时检查时间戳$TS_2$，保证签名消息的新鲜性。

③当验证成功后，完成 MN 对接入网络的认证，实现双向认证。

④为了提高切换效率，MN 收到 BA 后，先完成绑定更新过程，恢复与 CN 的连接然后验证签名消息以及更新公钥列表。

⑤按照移动节点所在位置，将移动节点移动接入过程分为两种情况：当移动节点从一个 MAP 域移动到另一个 MAP 域时，需要重新向 HA 发全局绑定更新消息。当移动节点在同一个 MAP 域内移动时，由于之前 MN 已经获得该 MAP 的签名，因而 MN 在 MAP 域内移动时可减少一次签名/验证过程。

4 分析及评价

本节从处理时延和信令开销两个方面将 CPK-IBS-IPv6 与 DAMIPv6[3]，HAMIPv6[4]，2-IBS-FAMIPv6[5] 进行比较，并对 CPK-IBS-IPv6 的安全性进行证明。

4.1 处理时延对比分析

定义认证时延为 MN 从移动到新的访问域并认证发出第一个路由宣告包到在新访问域收到 BA 消息完成绑定更新为止的一段时间间隔。

设 RSA 一次完整的签名和验证的时间为 $tRSA$，根据文献[11,12]分析，计算 512b 的双线性对加上 2 次点乘和 1 次 Hash 所需时间大约是计算 1024b 模指数的 3.5 倍。另外，计算 p 长度为 160b 的椭圆曲线上的点乘所需时间与计算 1024bRSA 模 n 指数运算所需时间相当[12]。CPK 签名验证算法的开销与 RSA 算法相比可忽略不计[13]。根据各种签名验证机制涉及的运算类型如表 1 所列。考虑 IBS-F 的预计算[1]，由表 1 可得到下面的结论：

$$t_{s\text{-}CPK\text{-}IBS\text{-}MN}=2tRSA \tag{1}$$

$$t_{s\text{-}CPK\text{-}IBS\text{-}HA}=2tRSA,t_{v\text{-}CPK\text{-}IBS}=2tRSA \tag{2}$$

$$t_{s\text{-}ACGA}=2tRSA,t_{v\text{-}ACGA}=2tRSA \tag{3}$$

表 1 CPK-IBS 方案的安全机制分析

IBE 方案的名称	Bilinear Pairings	Scale Multiplication	Point Addition	Others
CPK-IBS-HA Signing	0	1	0	Hash 1
CPK-IBS-MN Signing	0	1	0	Hash 1
CPK-IBS Verifying	1	0	1	NULL
ACGA Signing 1)	0	1	0	Hash 1
ACGA Verify	1	0	1	NULL

定义消息发送时延为消息发出和传输总时延：无线端传输延时 a(MN 与 AR 之间)、同一域内两节点间传输延时 b(AR 与 MAP 之间)和访问域与家乡域之间传输延时 c(MAP 与 HA 之间)。在 DAMIPv6，HAMIPv6，2-IBS-HAMIPv6 和 CPK-IBS-HAMIPv6 三个协议都实现双向认证的前提下，所需的总切换延时由式(4)－式(6)给出：

$$T_{DAMIPv6}=6a+8b+6c+21tp+2tRSA \tag{4}$$

$$T_{HAMIPv6}=4a+10b+4c+19tp+2tRSA \tag{5}$$

$$T_{2\text{-}IBS\text{-}HAMIPv6}=2a+b+3tp+t_{2-s}+\max(2c+4tp+b+t_{2-v},t_{1-s}+b+tp) \tag{6}$$

$$T_{CPK\text{-}IBS\text{-}HAMIPv6}=\max(2a+b+3tp+t_{MN-s},a+b+2c+3tp+t_{HA-s})+\max(tp+b+t_v,t_{MN-s}+b+tp) \tag{7}$$

为了具体分析 DAMIPv6，HAMIPv6，2-IBS-HAMIPv6 和 CPK-IBS-HAMIPv6 之间的性能，定义模型中的具体参数值：$a=4$ms，$b=2$ms，$tp=0.5$ms，令 $t_{s\text{-}HA\text{-}CPK\text{-}IBS}=2tRSA$，$t_{s\text{-}MN\text{-}CPK\text{-}IBS}=2tRSA$，$t_{v\text{-}CPK\text{-}IBS}=2tRSA$，最后得到 4 种方案的数学期望为：

$$E(\theta)=56.5+2t+3H \tag{8}$$

$$E(\omega)=49.5+2t+2H \tag{9}$$

$$E(\delta)=17.5+8t+H \tag{10}$$

$$E(\varphi)=\max(11.5+2t,9.5+H+2t)+2.5+2t \tag{11}$$

如图 3 所示，一方面签名/验证算法的本机处理时间确定时，会随着访问域与家乡域之间传输延时的增加而增加。在 CPK-IBS-HAMIPv6 方法中，MN 进入新访问域并请求 MAP 接入认证时实现 MN 与 MN 家乡域的 HA 交互，获得 HA 的认证，减少了与家乡域的交互带来的传输延时。当 H 小于 2ms 时候，CPK-IBS-HAMIPv6 的签名/验证处理延时只随着 t 值的变化而改变；当 H 大于 2ms 时，CPK-IBS-HAMIPv6 随着 H 的增大而增加。由图 3 分析可知，DAMIPv6 的切换延时增长幅度最大，当两地最大传输延时达到 40ms 时，DAMIPv6 的切换延时最大，接近 180ms，而 CPK-IBS-HAMIPv6 的切换延时只有 54ms。另一方面随着节点处理性能的降低，即签名/验证处理延时(t 值)的增加，2-IBS-HAMIPv6 的切换延时增长幅度最大，CPK-IBS-HAMIPv6 的切换延时增长幅度最小，当 t 足够大时，2-IBS-HAMIPv6 的增长幅度约为 CPK-IBS-HAMIPv6 的两倍。因此，当访问网络远离家乡网络时，本文提出的并发认证方法能显著降低移动 IPv6 网络 MN 移动切换过程中的“接入认证＋家乡注册”的切换延时。

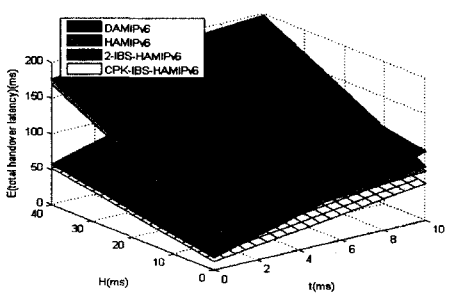

图 3 总切换延时的数学期望(不同 MAP 域间移动)

4.2 安全性证明

我们考虑 4 个安全概念：节点私钥的机密性、会话密钥的正确性、会话密钥的不可伪造性、会话密钥机密性保护和密钥托管，并证明基于 CPK_IBE 的可认证的密钥协商方案满足上述安全性需求。

4.2.1 私钥的保密性

在 CPK 机制下，私钥的保密性建立在 SSK 以及映射算

1) 当 MN 在子网间频繁移动时，通过减少家乡代理部分计算来减少签名阶段的点乘运算次数。

法函数 F 被安全保护的基础上。私钥一经产生则通过保密通道或安全物理信道交由用户秘密保管。函数 F 可由一些可变因子进行保护，如 F 取为 Hash 函数时输入秘密的初始值，或用硬件实现 F 等。

攻击 CPK 机制的可能方法之一是通过合谋算出私钥方程组，解出私钥因子。对于规模为 $l\times h$ 的私钥因子矩阵，私钥 SK 与私钥因子 $r_{i,j}^0$ 和 $r_{i,j}^1$ 呈线性关系。假定有 l 个双私钥已经泄露，则可建立 l 个关于私钥因子 $r_{i,j}^0$ 和 $r_{i,j}^1$ 的线性方程。若攻击者通过合谋获得 $m<l\times h$，则一般很难求出私钥因子 $r_{i,j}^0$ 的准确解，因此少量私钥的泄漏不会对系统的安全性造成影响。对于攻击者的合谋，可通过扩大 SSK 的规模或者定期更换 SSK 并更新用户私钥加以解决。

对于基于 CPK 的 IBS 的签名，根据第 3 节密钥生成机制可知，移动节点的私钥 SK_{ID} 由 SK_{ID}^0 和 SK_{ID}^1 两个部分构成，分别由 HA 和 MN 保管。HA 虽然拥有部分私钥 SK_{ID}^0，但无法获得 MN 保管的部分私钥 SK_{ID}^1，因而无法得到 S_{ID}。对于其他节点来说，只能公开参数 $params$ 中已知 P_{ID}，但由于计算群 G 上的 DH 问题是难的，其他节点无法通过 PK_{ID} 计算出 SK_{ID}。因此，任一实体私钥只有 PKG 知道，其他实体包括 HA 都无法获得。

4.2.2 签名的不可伪造性

本节采用随机预言机模型证明 3.2 节设计的 IBS 机制的安全性，即满足适应性选择消息攻击下的不可伪造性。令敌手 A 表示一个概率多项式时间的图灵机，输入为 IBS 机制的公开参数$\langle G_1,G_2,\hat{e},P,H_1,p,q\rangle$，其中 $q\geqslant 2^l$，$l=160$。

定义 1[12]（椭圆曲线离散对数问题 ECDL P） 给定定义于有限域 Fp 上的椭圆曲线 Ep 和 Ep 上的两点 $P,Q\in Ep$，寻找一个整数 d 使得在 Ep 中有 $dP=Q$。

定理 1 假设攻击者 A 可以在时间 t 内以优势 $\varepsilon\geqslant 10(n_1+1)(n_1+n^2)/2^l$ 产生一个存在性伪造签名，则存在另一个概率算法在时间 $t'\leqslant 120686n_2t/\varepsilon$ 范围内解决 G_1 群上的 ECDLP 问题。

证明：假设存在攻击者 A 在适应性选择消息和攻击下，能在时间 T 内以不可忽略的优势 $Adv_{\theta,A}=\varepsilon$ 模拟一个未签名消息 M 的有效签名(M,r,H,s)，则根据分叉引理[14,15]，必然存在另一个概率算法 B，在时间 $t'\leqslant 120686n_2t/\varepsilon$ 范围内以不可忽略的优势产生两个有效签名(M,r,H,s)，(M,r,H',s')，其中 $H\neq H'$，根据签名算法有：

$$\hat{e}(P,\sigma)=\hat{e}(PK_{ID},H_1(M)) \tag{12}$$

$$\hat{e}(P,\sigma)=\hat{e}(P,H_1(M)\times SK_{ID}) \tag{13}$$

$$\frac{\hat{e}(P,\sigma)}{\hat{e}(P,\sigma')}=\frac{\hat{e}(PK_{ID},H_1(M))}{\hat{e}(PK_{ID},H'_1(M))} \tag{14}$$

$$\frac{\hat{e}(P,\sigma)}{\hat{e}(P,\sigma')}=\frac{\hat{e}(P,H_1(M)SK_{ID})}{\hat{e}(P,H'_1(M)SK_{ID})} \tag{15}$$

$$\hat{e}(P,\sigma-\sigma')=\hat{e}(P,(H_1(M)-H'_1(M))\cdot SK_{ID}) \tag{16}$$

$$\hat{e}(P,\sigma-\sigma')\hat{e}(P,(H_1(M)-H'_1(M))\cdot SK_{ID})^{-1}=1 \tag{17}$$

令$(\sigma-\sigma')-(H_1(M)-H'_1(M))\cdot SK_{ID}=\lambda RP$，则式(17)得$\hat{e}(P,P)^{\lambda R}=1$，进而有 $\lambda R\equiv 0(\bmod q)$。因此，

$$SK_{ID}=\frac{\sigma-\sigma'}{H_1(M)-H'_1(M)} \tag{18}$$

$$(\sigma-\sigma')-(H_1(M)-H'_1(M))\cdot SK_{ID}=0(\bmod q) \tag{19}$$

最终，算法 B 输出 $PK_{ID}=SK_{ID}P$，根据定义 1，给定有限域 Fp 上的椭圆曲线 E 和 E 上的两点 PK_{ID}，P 输出 SK_{ID}，使得 $PK_{ID}=SK_{ID}P$，即在时间 $t'\leqslant 120686n_2tP\varepsilon$ 内解决了 ECDL P，证毕。

4.2.3 数据传输的安全性

在无线移动环境中，移动协议消息和认证消息的传输可以建立在安全关联之上，受安全关联 SA 的保护。由于 SA 是基于端到端的，任何需要传输信令消息的两个节点间，如 MAP 与 AAAv 之间，AAAv 与 AAAh 之间，AAAh 与 HA 之间，都需要建立一对 SA。同时，基于 CPK-IBS 的安全性，攻击者不能伪造签名消息，能够有效防止中间人攻击。由于签名消息是通过 HA 和 MN 的双私钥签名实现的，从而能够有效防止消息重放攻击。

4.2.4 签名的新鲜性

在 FAMIPv6 和 IBS-FAMIPv6 方案中，应采用时间戳来保证签名的新鲜性，否则，验证者不能确定签名产生的确切时间，也就无法验证签名的有效性。而在 CPK-IBS-IPV6 方案中，一旦一个私钥被吊销，它就永远不能再被用于签名。因此，验证者若获得了一个数字签名，那么也就意味着在签名生成时刻，签发者的私钥经过 HA 认证是合法的。

4.2.5 即时身份撤销

在传统的 IBS 中，由于需要定期发布被吊销签名的公钥，往往会有时间延迟。在这期间，证书仍然被认为是合法的，这是一个明显的安全问题。在本方案中，一旦需要撤销一个用户的权利，那么只需要在 HA 端及时使相应的私钥失效就可以实现身份撤销。

4.2.6 密钥托管

由于移动节点的部分是 PKG 生成的，只有 PKG 知道公私钥对。由于不知道移动节点的部分私钥，即使是不诚实的 HA 也不能够获得节点完整的私钥，因此不能冒充节点解密密文或者伪造签名。而且在 HA 和节点之间也不需要安全的密钥分发信道，部分密钥的丢失不会影响系统的机密性。本方案提供了节点最终的密钥保护。

结束语 本文提出了一种 MIPv6 网络接入认证方法，并设计了基于 CPK 和 IBS 的签名和验证方案，降低了签名验证算法的时间复杂度，解决了移动节点的密钥托管问题。其应用于本方案的认证阶段，高效地实现了用户与网络的双向认证。另外，该方法利用分层身份签名技术的特点，将层次化移动切换过程和认证过程进行有机整合，减少了访问网络与家乡网络之间的延时。分析结果表明，本方案在总认证切换时延和信令开销方面表现出比现有方案更好的性能。

参 考 文 献

[1] Kim C, Kim Y S, Huh E N, et al. Performance improvement in mobile IPv6 using AAA and fast handoff[C]// Proceedings of the International Conference on Computational Science and It's Applications (ICCSA'04). LNCS 3043. Heidelberg: Springer-Verlag, 2004: 738-745

[2] Gergiades M, Akhtar N, Politis C, et al. AAA context transfer for seamless and secure multimedia services over All IP infra-

structures[C]//Proceedings of the 5th European Wireless Conference (EW'04). Barcelona,2004:442-448

[3] Le F,Patil B,Perkins C E,et al. Diameter mobile IPv6 application. Internet IETF Draft (working in progress)

[4] Engelstad P, Haslestad T, Paint F. Authenticated access for IPv6 supported mobility[C]//Proceedings of the IEEE International Symposium on Computers and Communication (ISCC'03). Kemer-Antalya,2003:569-575

[5] 田野,张玉军,刘莹,等. 移动 IPv6 网络基于身份的快速认证方法[J]. 软件学报,2006,17 (9):1980-1988

[6] 田野,张玉军,张瀚文,等. 移动 IPv6 网络基于身份的层次化接入认证机制[J]. 计算机学报,2007,30(6):905-915

[7] Katz J,Wang N. Efficiency Improvements for Signature Scheme with Tight Security Reductions [C] // ACM-CCS' 2003. Washington,DC,USA:ACM,2003. 155-164

[8] 南相浩. CPK 标识认证[M]. 北京:国防工业出版社,2006:186-210

[9] Boneh D,Lynn B,Shacham H. Short Signatures from the Weil Pairing[C]//Advance in Cryptology-ASIACRYPT 2001,LNCS 2248. Gold Coast,Australia:Springer Verlag. 2001:213-229

[10] Soliman H,Castelluccia C,Malki K E,et al. Hierarchical Mobile IPv6 mobility management (HMIPv6). IETF Internet Draft (working in progress),2003

[11] Barreto PSLM,Kim H Y,Lynn B,et al. Efficient algorithms for pairing-based cryptosystems [C] // Advances in Cryptology Crypto'02. LNCS 2442. Heidelberg:Springer-Verlag,2002:354-368

[12] Galbrait S,Harrison K,Soldera D. Implementing the Tate pairing[C]//Proceedings of the Algorithm Number Theory Symposium. LNCS 2369. Heidelberg:Springer-Verlag,2002:324-337

[13] 毛文波. 现代密码学理论与实践[M]. 北京:电子工业出版社,2004

[14] Pointcheval D,Stern J. Security proofs for signature Scheme[C]//Advances in Cryptology-Eurocrypt 1996. LNCS 1070. Heidelberg:Springer-Verlag,1996:387-398

[15] Pointcheval D,Stern J. Security argument s for digital signature and blind signature[J]. Journal of Cryptology,2000,13(3):361-396

(上接第 4 页)

[16] Björklund A,Husfeldt T,Khanna S. Approximating longest directed paths and cycles[C]//Proc. 31th International Colloq (ICALP). Automata,Languages and Programming,2004

[17] Gabow H N. Finding paths and cycles of superpolylogarithmic length[C]//Proc. 36th STOC. 2004

[18] Papadimitriou C,Yannakakis M. On limited nondeterminism and the complexity of the V-C dimension[J]. Journal of Computer and System Sciences,1996,53:161-170

[19] Downey R,Fellows M. Fixed parameter tractability and completeness. Complexity Theory: Current Research [M]. Cambridge University Press,1992

[20] Schmidt J P,Siegel A. The spatial complexity of oblivious k-probe hash functions[J]. SIAM Journal on Computing,1990,19 (5):775-786

[21] Bodlaender H L,Downey R G,Fellows M R,et al. On problems without polynomial kernels [C] // Proc. 35th ICALP. volume 5125 of LNCS,Springer,2008:563-574

[22] Alon N,Yuster R,Zwick U. Color-coding[J]. J. ACM,1995,42 (4):844-856

[23] Fellows M R,Knauer C,Nishimura N,et al. Faster fixed parameter tractable algorithms for matching and packing problems[C]//Lecture Notes in Computer Science 3221,(ESA 2004). 2004:311-322

[24] Chen Jianer. Parameterized computation and complexity:a new approach dealing with NP-hardness[J]. Journal of Computer Science and Technology,2005,20:18-37

[25] Chen Jianer, Lu Songjian, Sze Sing-Hoi, et al. Improved algorithms for path, matching, and packing problems[C]//Proceedings of ACM-SIAM Symposium on Discrete Algorithms (SODA). 2007:298-307

[26] Kneis J, Mölle D, Richter S, et al. Divide-and-color[C]//Proceedings of the International Workshop on Graph-Theoretic Concepts in Computer Science (WG). LNCS 4271, Springer, 2006:58-67

[27] Chen J,Kneis J,Lu Songjian,et al. Randomized Divide-and-Conquer Improved Path,Matching,and Packing Algorithms[manuscript]. 2008

[28] Koutis I. Faster algebraic algorithms for path and packing problems[C]//Proceedings of the International Colloquium on Automata, Languages and Programming (ICALP). LNCS 5125, Springer,2008:575-586

[29] Williams R. Finding paths of length k in $O*(2^k)$ time. arXiv:0807. 3026. July 2008

[30] Naor M,Schulman L,Srinivasan A. Splitters and near-optimal derandomization[C]//Proc. 36th IEEE Symp. on Foundations of Computer Science (FOCS 1995). 1995:182-190

[31] Chen J. Randomized Disposal of Unknowns and Implicitly Enforced Bounds on Parameters[C]//IWPEC. 2008:1-8

[32] Bulterman R W,van der Sommen F W,Zwaan G,et al. On computing a longest path in a tree[J]. Information Processing Letters,2002,81:93-96

[33] Uehara R, Uno Y. Efficient algorithms for the longest path problem[C]//Proc. 15th Annual International Symposium on Algorithms and Computation. volume 3341 of Lecture Notes in Computer Science,Springer-Verlag,2004:871-883

[34] Uehara R,Valiente G. Linear Structure of Bipartite Permutation Graphs and the Longest Path Problem[J]. Information Processing Letters,2006

[35] Uehara R,Uno Y. On Computing Longest Paths in Small Graph Classes[J]. Int. J. Foundations Comput. Science,2007,18:911-930

[36] Liu Y,Lu S,Chen J,et al. Greedy localization and color-coding: improved matching and packing algorithms[C]//Proc. 2nd International Workshop on Parameterized and Exact Computation. Lecture Notes in Computer Science 4169,2006:84-95