移动 IPv6 网络基于身份的层次化接入认证机制

田 野[1),2)] 张玉军[1)] 张瀚文[1),2)] 李忠诚[1)]

[1)](中国科学院计算技术研究所 北京 100080)

[2)](中国科学院研究生院 北京 100039)

摘 要 设计了一种基于身份的层次化签名方案,并在该方案基础上提出了一种适用于移动 IPv6 网络环境的层次化接入认证方法.该方法使用分级 NAI(Network Access Identifier)作为公钥,简化了无线移动环境中的密钥管理;利用层次化思想对接入认证和移动注册进行层次化管理,减少了切换认证处理流程;基于签名机制实现了用户与接入网络的双向认证.作者用设计的切换延时分析模型,对该方法和几种传统方法进行了比较,证明当移动节点远离家乡域及在一定范围内频繁微移动时,该方法比传统方法的效率更高.通过安全性分析证明了该方法在一定程度上实现了私钥的保密性、签名的不可伪造性等功能.最后还讨论了该方法的一种可扩展变形,用于实现多级层次化移动 IPv6 框架下的接入认证.

关键词 移动 IPv6 网络;接入认证;基于身份签名;快速切换

中图法分类号 TP393

Identity-Based Hierarchical Access Authentication in Mobile IPv6 Network

TIAN Ye[1),2)] ZHANG Yu-Jun[1)] ZHANG Han-Wen[1),2)] LI Zhong-Cheng[1)]

[1)](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080)

[2)](*Graduate University of Chinese Academy of Sciences, Beijing* 100039)

Abstract Access authentication is very important to deploy mobile IPv6 networks. This paper proposes a hierarchical access authentication method for mobile IPv6 network, which is based on a hierarchical identity based signature scheme. This method adopts multilevel NAI(Network Access Identifier) as public key to simplify key management in wireless mobile environment, utilizes hierarchical authentication and mobile registration to decrease handover authentication process and implements mutual authentication between terminal and access network based on signature scheme. A handover latency analytical model is proposed to show that the proposed scheme is more efficient than others, especially in the conditions that terminal is further from home domain and moves frequently. Security analysis shows that the proposed scheme is sufficient for private-key privacy, signature unforgeability and so on. At last a scalability version is discussed, which is applied to realize access authentication in multi-hierarchical mobile IPv6.

Keywords mobile IPv6; access authentication; identity based signature; fast handover

1 引 言

在无线移动 IPv6 网络中,一方面,用户需要在任意位置接入网络,由于移动互联网的开放特性增大了潜在的安全威胁,从保障网络安全可靠运营的角度,每一个接入网络必须对接入的移动节点实施认证.另一方面,为了给接入用户提供诸如视频点播

收稿日期:2005-08-17;修改稿收到日期:2006-12-26.本课题得到国家自然科学基金(90604014)资助.**田 野**,男,1979 年生,博士,主要研究方向为下一代互联网、无线移动网络安全.E-mail: tianyeict@gmail.com.**张玉军**,男,1976 年生,博士,副研究员,主要研究方向为下一代互联网、移动计算.**张瀚文**,女,1981 年生,博士研究生,主要研究方向为下一代互联网、无线移动网络.**李忠诚**,男,1962 年生,博士,研究员,主要研究领域为计算机网络、可信计算.

等实时应用,保障移动环境的切换效率是无线移动IPv6网络必须解决的问题.由于移动切换和接入认证往往同时进行,在切换过程中加入认证过程会进一步影响切换效率.随着各种实时应用的增加,必须最大程度地减少用户切换和接入认证的延时与开销,对接入控制技术的研究已成为移动IPv6网络安全、可靠、高效运营的重要基础.

AAA(Authentication, Authorization and Accounting)技术(如Diameter协议)正是为了解决接入用户身份认证、授权和记账问题而提出的.但是,AAA协议最初只是针对有线环境提出的一种实现对终端设备接入认证的框架,并没考虑到接入方式不同带来的差异.于是有研究提出了在无线环境中,如何结合移动IPv6(Mobile IPv6,MIPv6)技术和AAA技术解决安全性问题的方法[1].

为了解决在切换过程中引入认证会增加切换延时的问题,国内外也提出了一些解决方案,归纳起来主要包括以下几类:基于消息捎带的策略[1],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[2],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[3],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[2,4],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,也没有过多考虑到加入接入认证过程后给切换延时带来的影响到底在哪里,如何最大程度地消除这种影响.这些策略大多忽略了具体认证方法的实现,而这恰恰是决定认证性能的关键所在.而且,现有认证机制中采用的支持双向认证的认证方法,大多数是基于公钥证书实现的[5].而证书机制需要一个基本的前提假设:即所有证书都是公开的、普遍存在的,对于每个人来说都是能很容易使用的.由于无线移动环境下终端用户的移动性特点,使得终端用户无法确知接入网络证书中心的地址,因而不能有效获得接入网络的公钥证书.于是,文献[6]提出了一种无线移动IPv4环境中基于身份加密的AAA认证方法.基于身份的密钥方案通过构建身份与公钥之间一对一映射,简化了公钥的获取,从而消除了对公钥证书和认证中心的依赖.该方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,而且也没能解决基于身份密码方案固有的密钥托管问题.

本文设计了一种基于身份的层次化签名方案,并在此基础上提出了一种适用于移动IPv6网络环境的层次化接入认证机制.该机制利用基于身份层次化签名方案的特性,将层次化移动切换过程和认证过程进行有机整合,提高整体性能.同时,该机制是建立在DH(Diffie-Hellman)问题基础上的,具有足够的安全性.本文第2节简单介绍基于身份的密码方案;第3节给出一种2层身份签名机制设计方案,并重点阐述基于2层身份签名的层次化认证方案;第4节给出相应的性能分析、安全性分析和可扩展性分析;最后总结本文并给出下一步工作.

2 基于身份的密码方案

基于身份的密码方案(Identity-Based Cryptography,IBC)最初是为解决公钥证书方案中密钥管理复杂等问题由Shamir于1984年提出的[7],包括基于身份加密(Identity-Based Encryption,IBE)和基于身份签名(Identity-Based Signature,IBS)两种机制.该方案允许用户公钥可以是与用户任意身份信息(如e-mail或其他)相关的一个二进制流.该方案中包括一个可信任的授权机构——私钥产生方(Private Key Generator,PKG),完成根据用户身份信息计算对应私钥的功能.

Shamir虽然提出了IBC的想法,但并没能给出一种实用的实现方案.直到2001年,Boneh和Franklin应用超奇异椭圆曲线上的对技术(Weil对或Tate对)建立了第一个实用的基于身份的公钥密码体制[8].为了解决IBC机制无法应用于大规模网络环境的问题,Horwitz和Lynn基于BF机制提出了层次化IBC的概念[9],随后Gentry和Silverberg在文献[10]中提出了第一个安全且实用的层次化基于身份的加密(Hierarchical IBE,HIBE)机制.之后Boneh等人从效率方面对HIBE做了进一步研究[11],提出了固定密文长度的HIBE机制.

2.1 双线性对(Bilinear Pairing)

令$(\mathbb{G},\cdot)$和$(\mathbb{G}_1,\cdot)$为两个阶为素数p的循环加法群,$g\in\mathbb{G}$是$\mathbb{G}$的生成元.双线性对就是$\hat{e}:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_1$,该对满足如下性质:

① 双线性.对于所有的$P,Q\in\mathbb{G}$,所有的$a,b\in\mathbb{Z}$,满足$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$.

同时对任意$P_1,P_2,Q\in\mathbb{G}$,有

$\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\times\hat{e}(P_2,Q)$,

或者对任意 $P,Q_1,Q_2\in\mathbb{G}$，有

$$\hat{e}(P,Q_1+Q_2)=\hat{e}(P,Q_1)\times\hat{e}(P,Q_2).$$

② 非退化性. $\hat{e}(g,g)\neq 1$.

③ 可计算性. 对于所有的 $P,Q\in\mathbb{G}$，存在一种有效算法计算 $\hat{e}(P,Q)\in\mathbb{G}_1$.

2.2 HIBS 机制框架

一个 IBS 机制由 4 个算法组成：Setup，Extract，Sign 和 Verify. 其中 Setup 和 Extract 由 PKG 执行. PKG 根据安全参数 k，执行 Setup 算法产生主密钥和公开参数；Extract 用于生成任意给定用户身份 ID 的私钥；算法 Sign 由签名者执行，生成对某消息的签名；Verify 由任一验证者执行，验证签名消息的真伪.

对于层次化机制，PKGs 和用户组成一棵树，身份由一个向量组表示. 一个 ℓ 维向量表示第 ℓ 层用户/PKGs 的身份，用 ID 多元组表示：$ID|\ell=\{ID_1,\cdots,ID_\ell\}$. HIBS 的 4 个算法与 IBS 的类似，除了在 Extract 算法中，HIBS 生成给定身份 ID 的私钥时，ID 可能是某个用户的，也可能是低层 PKG 的. 第 ℓ 层身份 ID 的私钥用 $S_{ID|\ell}$ 表示. HIBS 的 4 个算法具体描述如下：

Setup. 基于安全参数 k 生成公开参数 $params$，包括消息空间和签名空间的描述，随机选择主密钥 s，并秘密保存.

Extract. 根据输入的身份 ID，利用主密钥(根 PKG)或 $S_{ID|j-1}$(低层 PKGs，若 ID 是第 j 层)生成私钥 $S_{ID|j}$.

Sign. 基于输入$(m,S_{ID|j})$，生成签名 σ.

Verify. 基于输入(σ,m,ID)，根据 $params$，验证签名 σ 的真伪. 真，输出 T；假，输出 F.

3 层次化认证方法

在移动 IPv6 中，MN 每次移动都要执行绑定更新(Binding Update，BU)，如果 MN 远离家乡，这将会带来很大的延时和开销. 为了解决这个问题，人们提出了本地化移动方案，又称层次化位置登记策略[12]. 它的基本思想是采用层次化移动管理，引入移动锚点(Mobility Anchor Point，MAP)，并对 MN 的操作做微小的改动，而对家乡代理(Home Agent，HA)和通信节点(Correspondent Node，CN)并没有任何影响. 在这种策略中，每一个 MAP 管理着若干访问路由器(Access Router，AR)，这些 AR 不断地广播有关 MAP 信息. 当 MN 进入一个 MAP 域(MAP 所管辖的范围)后，根据接收地信息，它首先形成一个本地链路地址，并向 MAP 进行本地注册. MAP 扮演本地 HA 的角色，它以 MN 的名义接受分组，通过封装将这些分组转发给 MN. MN 可以通过 HA 或者直接与 CN 进行通信. 当 MN 在同一个 MAP 域运动时，如果它移出当前链路，只需执行本地注册；只有当它从一个 MAP 域移动到另一个 MAP 域时，它才向 HA 和 CN 注册.

另外，现有认证框架完成认证(单向或双向)需要 MN 与认证服务器之间的多次交互，认证延时将随着交互次数的增多而显著增大. 根据签名机制的特点，一次交互完成后，签名/验证过程也同时完成，我们可以通过一次交互就能完成 MN 与接入网络的双向认证，从而减少了接入认证过程的传输时延.

基于上述分析和考虑，本节设计了一种深度为 2 的层次化身份签名方案，并在此基础上，提出了一种层次化认证机制，有效实现了用户与接入网络的双向认证.

3.1 2 层身份签名机制

Root Setup. 根 PKG 执行如下步骤：

1. 基于安全参数 k 生成阶为素数 q 的循环群 $\mathbb{G}$，$\mathbb{G}_1$ 以及双线性对 $\hat{e}:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$；

2. 随机选择生成元 $P_0\in_U\mathbb{G}$；

3. 随机选择整数 $s_0\in_U\mathbb{Z}_q^*$，计算 $Q_0\leftarrow s_0P_0$；

4. 选择杂凑函数 $H_1:\{0,1\}^*\to\mathbb{G}$ 和 $H_2:\{0,1\}^*\to\mathbb{G}$.

消息空间 $\mathcal{M}=\{0,1\}^*$，签名空间 $\mathcal{S}=\mathbb{G}^2$，公开参数 $params=(\mathbb{G},\mathbb{G}_1,\hat{e},P_0,Q_0,H_1,H_2)$，根 PKG 的私钥是 s_0.

Level-1 Setup. 第 1 层 PKG 随机选择 $s_1\in_U\mathbb{Z}_q^*$，秘密保存.

Level-1 PKGs Extract. 设第 1 层 PKG 身份 ID 为 1 元组 I_1，令 S_0 是 $\mathbb{G}$ 的单位元. 则根 PKG 执行如下操作生成 I_1 对应的私钥：

1. 计算 $P_1\leftarrow H_1(I_1)\in\mathbb{G}$；

2. 计算该身份 ID 对应私钥 $S_1\leftarrow s_0P_1$.

Level-2 Users Extract. 设第 2 层用户身份 ID 为 2 元组(I_1,I_2). 则该用户的父亲执行如下操作生成(I_1,I_2)对应的私钥：

1. 计算 $P_2\leftarrow H_1(I_1\|I_2)\in\mathbb{G}$；

2. 计算该身份 ID 对应私钥 $S_2\leftarrow S_1+s_1P_2$；

3. 计算 $Q_1\leftarrow s_1P_0$.

将结果集(S_2,Q_1)返回给该用户.

Sign. 签名者随机选择 $s_2\in_U\mathbb{Z}_q^*$ 并秘密保存，用身份(I_1,I_2)对消息 $M\in\mathcal{M}$签名，需要执行如下步骤：

1. 计算 $P_M\leftarrow H_2(I_1\|I_2\|M)\in\mathbb{G}$；

2. 计算签名 $\sigma\leftarrow S_2+s_2P_M$；

3. 发送签名 σ 和$(Q_2\leftarrow s_2P_0)$给验证者.

Verify. 设$\langle\sigma,Q_2\rangle\in\mathcal{S}$是身份$(I_1,I_2)$对消息 M 的签名，则验证者判定等式

$$\hat{e}(P_0,\sigma)=\hat{e}(Q_0,P_1)\cdot\hat{e}(Q_1,P_2)\cdot\hat{e}(Q_2,P_M)\quad(1)$$

是否成立.若成立,则输出 T;否则输出 F.

3.2 层次化认证框架

在现有认证机制中,MN 认证信息存放在家乡网络,对 MN 的接入认证必须通过与家乡网络认证服务器的交互来实现,因而认证延时将随着访问网络与家乡网络之间距离的增加而显著增大.根据 IBS 机制的实现原理,签名/验证功能的实现仅取决于签名参数,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,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.

系统具体实现框架如图 1 所示.整个系统由一个根 PKG、若干第 1 层 PKG(MAPs 和 HA)和若干第 2 层用户(ARs 和 MN 等)组成.当 MN 接入新访问域时,只需在完成绑定更新的同时与接入的 AR 利用对发送消息的签名完成双向认证过程.

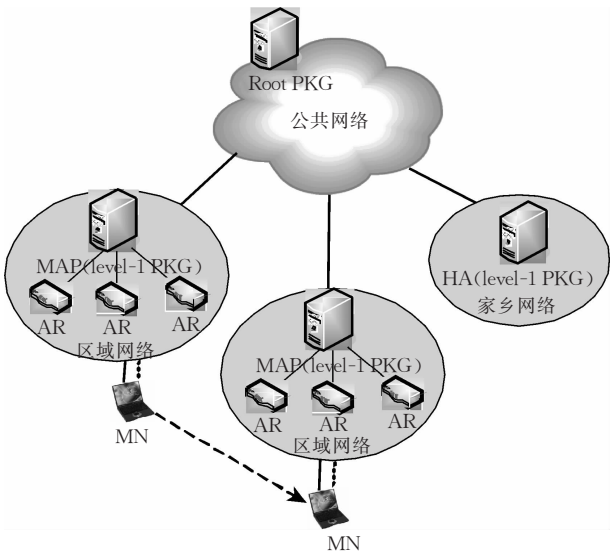


图 1 层次化接入认证机制框架

在描述协议的具体实现前,我们规定如下设计准则:

① 协议要求网络各实体均支持 2 层身份签名机制,如 HA,MAPs,ARs 和 MN.

② 根 PKG 生成公开参数

$$params=(\mathbb{G},\mathbb{G}_1,\hat{e},P_0,Q_0,H_1,H_2),$$

每个域内实体均能获得.

③ 公钥采用多级 NAI 标识.第 1 层 PKG 身份 ID 形如 domain.net,其中 MN 家乡网络身份 ID 为 domain0.net.第 2 层用户身份 ID 形如(domain.net, username@ domain.net),其中 MN 身份 $ID=$(domain0.net, mn@domain0.net).

④ 每一个网络实体维护一个 Q 值列表,存储第 1 层 PKG 身份 ID 及其公开的 Q 值.

⑤ 为了抵抗重放攻击,每个签名消息必须携带时间戳.

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,如图 2 所示.当移动节点在同一个 MAP 域内移动时,只需向 MAP 发本地绑定更新消息,而不需要与 HA 做任何交互,如图 2 灰框部分所示.具体描述如下:

(1) $\mathrm{MN}\rightarrow\mathrm{AR}_1$: $Req=\langle BU_{\mathrm{MAP}}\|BU_{\mathrm{HA}}\|TS_1\|\{BU_{\mathrm{MAP}}\|BU_{\mathrm{HA}}\|TS_1\}Sign_{\mathrm{MN}}\|Q_2\|ID_{\mathrm{MN}}\rangle$.

MN 获得 LCoA 和 RCoA 后生成 BU_{MAP} 和 BU_{HA} 消息,利用根 PKG 生成的公开参数 $params$、HA 生成的 Q_1,执行 2 层身份签名机制中的 Sign 算法,生成对绑定更新消息的签名以及 Q_2,并将绑定更新消息连同签名以及 Q_2 和身份 $ID_{\mathrm{MN}}=(I_1,I_2)$ 组成 Req 消息.

(2) $\mathrm{AR}_1\rightarrow\mathrm{MAP}$: $\langle BU_{\mathrm{MAP}},BU_{\mathrm{HA}},[\mathrm{QVR}]\rangle$.

① AR_1 首先查询自己的 Q 值列表,寻找是否存在 I_1 表项.若存在,则直接取出对应 Q_1,结合收到的 Q_2,执行 2 层身份签名机制中的 Verify 算法验证 $\{BU_{\mathrm{MAP}}\|BU_{\mathrm{HA}}\|TS_1\}Sign_{\mathrm{MN}}$,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 AR_1 对 MN 的认证.

② 若不存在,则向 MAP 发送 QVR 消息获取 I_1 对应的 Q 值.收到 QVA 消息后,先验证签名,再更新 Q 值列表.

③ 为了提高效率,AR_1 先查询 Q 值列表,然后发送 $\langle BU_{\mathrm{MAP}},BU_{\mathrm{HA}},[\mathrm{QVR}]\rangle$ 消息,最后验证签名,从而实现绑定更新与验证的并发执行.

(3) $\mathrm{MAP}\rightarrow\mathrm{HA}$: $\langle BU_{\mathrm{HA}}\rangle$.

① MAP 一旦收到 QVR 消息,首先查询 Q 值列表,寻找是否存在 I_1 表项.若存在,则生成 QVA 消息将 Q 值返回给 AR_1.然后对 MN 的 LCoA 进行绑定更新以及转发 BU_{HA}.

② 若不存在,则向 HA 发送 QVR 消息获取 Q 值.收到 QVA 消息后,先向 AR_1 转发 QVA,再更新 Q 值列表.

③ MAP 生成 BA_{MAP} 消息,并对公开的 Q_1' 用身份 $ID_{\mathrm{MAP}}=(I_1')$ 进行签名.

(4) $\mathrm{HA}\rightarrow\mathrm{MAP}$: $\langle BA_{\mathrm{HA}}\rangle$.

HA 若收到 QVR 消息，立刻回应 QVA 消息.

(5) MAP—>AR_1：$\langle BA_{MAP} \| BA_{HA} \| Q_1' \| TS_2 \| \{Q_1' \| TS_2\}\ Sign_{MAP}\rangle$.

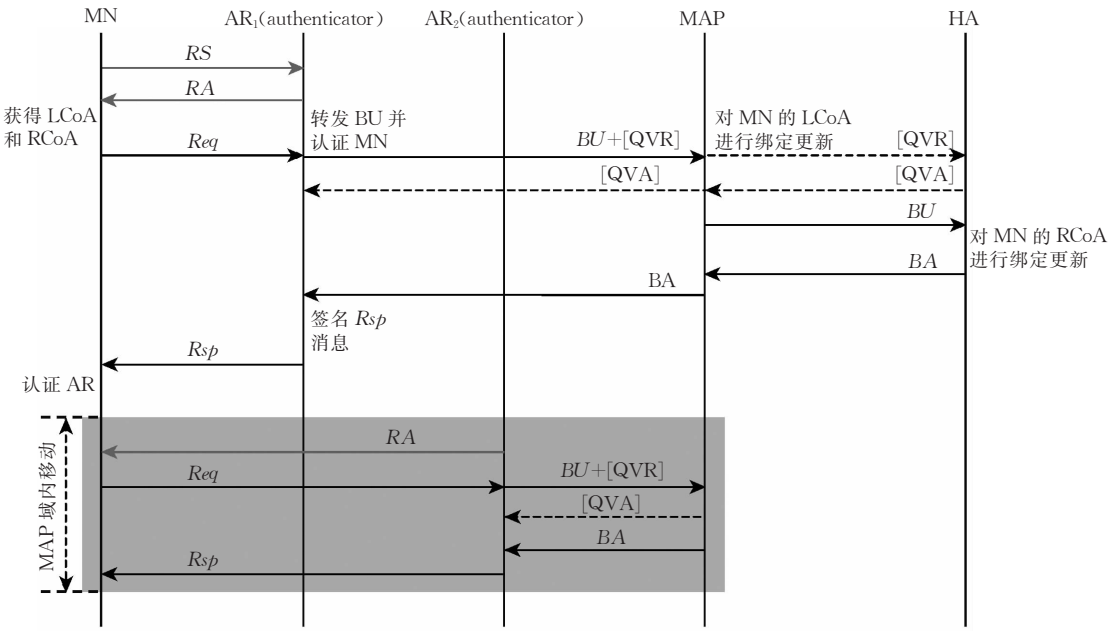
MAP 收到 HA 的 BA_{HA} 消息后，连同 BA_{MAP} 消息、Q_1' 以及对它们的签名发送给 AR_1.

(6) AR_1 —>MN：$Req=\langle BA_{MAP} \| BA_{HA} \| Q_1' \| Q_2' \| TS_2 \| TS_3 \| ID_{AR_1} \| \{Q_1' \| TS_2\} Sign_{MAP} \| \{BA_{MAP} \| BA_{HA} \| TS_3\} Sign_{AR_1}\rangle$.

① AR_1 使用 Q_1' 和自己的私钥对绑定确认消息进行签名，并生成 Q_2'，然后将绑定确认消息连同签名以及 Q_1'，Q_2'，$ID_{AR_1}=(I_1', I_2')$ 和收到的 MAP 的签名组成 Rsp 消息.

② MN 首先验证 MAP 对 Q_1' 的签名，同时检查时间戳 TS_2，保证签名消息的新鲜性. 然后验证 AR_1 的签名 $\{BA_{MAP} \| BA_{HA} \| TS_3\} Sign_{AR_1}$，同时检查时间戳 TS_3，保证签名消息的新鲜性. 验证成功，完成 MN 对接入网络的认证，实现双向认证.

③ 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 Q 值列表.



RS/RA: Router Solicitations/Advertisement
LCoA/RCoA: On-Link/Regional Care-of Address
Req: Registration-Request piggyback BU for MAP and HA and the signature of MN
BU/BA: Binding Update/Acknowledgement
Rsp: Registration-Response piggyback BA of MAP and HA and the signature of AR
QVR/QVA: Q-Value Request/Answer

图 2　基于身份签名的层次化认证协议

当 MN 在 MAP 域内移动时，设从 AR_1 到 AR_2，由于之前 MAP 已更新 Q 值列表，AR_2 只需向 MAP 发送 QVR 消息就可获得 Q_1. 另外，由于之前 MN 已经获得该 MAP 的 Q_1'，MAP 无需发送 Q_1' 及其签名，因而减少了一次签名/验证过程.

4　讨　论

4.1　性能分析

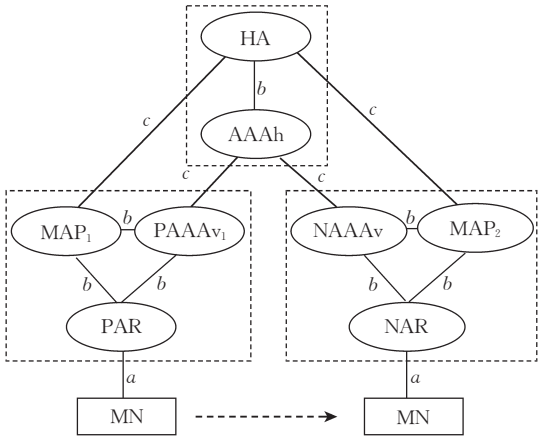
集成接入认证的切换效率对于移动 IPv6 网络的运行至关重要. 我们用基于文献[13]提出的切换延时性能分析模型(如图 3 所示)来比较本文提出的 2-IBS-HAMIPv6 协议、Le 等人提出被 IETF 公布为草案标准的 DAMIPv6 协议[1] 以及 Engelstad 等人提出的 HAMIPv6 协议[4] 的切换延时. 这里定义切换延时是从 MN 收到新访问域第一个路由宣告包开始，到 MN 在新访问域收到 BA 消息完成绑定更新为止的一段时间间隔.

DAMIPv6 协议[1] 将移动 IPv6 协议消息与 Diameter 协议消息进行了有机结合，减少了 MN 与家乡域的交互次数，一定程度上提高了移动性能. 该协议虽然采用了消息捎带机制，但只是将切换处理简单挪动到认证处理过程中，实际的绑定更新仍是在认证成功后进行. 同时认证过程基于挑战-应答方式，需要 MN 与家乡域的认证服务器经过多次交互才能完成认证. 当采用 RSA 签名算法实现认证时，至少需要 MN 与家乡域的认证服务器交互 2 次才能完成网络对用户的单向认证. 而若要实现双向认

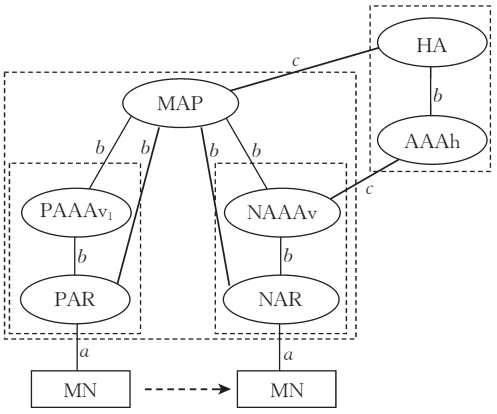
证,则需再增加一个来回.

HAMIPv6 协议[4]则是将层次化移动 IPv6 协议消息与 Diameter 协议消息进行了有机结合,通过 MAP 在路由宣告消息中捎带挑战字来减少挑战-应答方式的交互次数,从而在 MN 通过访问域认证服务器(AAAv)与家乡域认证服务器(AAAh)之间一次交互就可实现网络对 MN 的单向认证.然而,若要实现 MN 对网络的认证,该协议仍然需要再增加一个来回.

如图 3 所示,任意两实体间的传输延时被分为三类,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).由于传输延时与两实体间物理位置有关(与跳数成正比),而域内实体物理分布较固定且相距较近,可近似为一个固定值 b.但访问域与家乡域间传输延时将随着访问域具体位置的不同而变化,用变量 c 表示,且 $c \geq b$.另外,由于无线局域网诸如 802.11 系列协议最大带宽只有 11Mbps,有 $a > b$.在考虑接入认证后的移动切换延时除了传输延时和本机处理时间(设为 t_p)外,更重要的就是本机实现认证功能的处理时间,这与采用的具体认证算法以及节点机器配置(如 CPU、内存等)有关.因而评价移动切换延时将主要考虑两个变量,访问域与家乡域之间传输延时 c 和本机对认证算法的处理时间 t.设采用 RSA 签名机制"一次签名+一次验证"所需总时间为 t_{RSA},而采用 2-IBS 机制第 1 层和第 2 层用户签名/验证所需时间为 t_{1-s}/t_{1-v} 和 t_{2-s}/t_{2-v}.



(a) 不同 MAP 域间切换延时分析模型



(b) 同一 MAP 域内切换延时分析模型

图 3 延时分析模型

2-IBS 机制的处理性能主要由以下几个操作决定:椭圆曲线上的数乘和点加操作、群上乘法操作和 2.1 节定义的双线性对操作.根据 3.1 节介绍,2-IBS-HAMIPv6 机制的第 2 层用户签名阶段需要进行 2 次数乘,1 次点加和 1 次 Hash 运算,验证阶段需要 4 次双线性对运算和 2 次群上乘法运算,若预计算 $\hat{e}(Q_0, P_1)$,则只需要 3 次双线性对运算和 2 次群上乘法运算.而对于第 1 层 PKG 执行签名阶段则只需要 1 次数乘,1 次点加和 1 次 Hash 运算,执行验证阶段需要 3 次双线性对运算和 1 次群上乘法运算,若预计算 $\hat{e}(Q_0, P_1)$,则只需要 2 次双线性对运算和 1 次群上乘法运算.根据文献[14-15]分析,计算 512-b 的双线性对-Tate 对加上 2 次点乘和 1 次 Hash 所需时间大约是计算 1024-b 模指数的 3.5 倍.另外,计算 p 长度为 160-b 的椭圆曲线上的点乘所需时间与计算 1024-b RSA 模 n 指数运算所需时间相当[15].因此,我们可以得出如下结论:

$$t_{1-s} = 2t_{\mathrm{RSA}},\ t_{2-s} = 3t_{\mathrm{RSA}} \tag{2}$$

$$t_{1-v} = 3t_{\mathrm{RSA}},\ t_{2-v} = 5t_{\mathrm{RSA}} \tag{3}$$

当 MN 在不同 MAP 域间移动时,设新访问域的 NAR 和 MAP_2 均未知 MN 身份 ID 对应的 Q_1 值,MN 未知 MAP_2 身份 ID 对应的 Q_1' 值.DAMIPv6、HAMIPv6 和 2-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)~(6)给出:

$$T_{\mathrm{DAMIPv6}} = 6a + 8b + 6c + 21t_p + 2t_{\mathrm{RSA}} \tag{4}$$

$$T_{\mathrm{HAMIPv6}} = 4a + 10b + 4c + 19t_p + 2t_{\mathrm{RSA}} \tag{5}$$

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

假设 c 服从 $[b, H]$ 上的均匀分布,$t_{2-v} > t_{2-s} > t_{1-s} > t_p$,令 $E(\theta)$,$E(\omega)$ 和 $E(\delta)$ 分别表示 T_{DAMIPv6},T_{HAMIPv6} 和 $T_{\text{2-IBS-HAMIPv6}}$ 的数学期望,则

$$E(\theta) = 6a + 11b + 21t_p + 2t_{\mathrm{RSA}} + 3H \tag{7}$$

$$E(\omega) = 4a + 12b + 19t_p + 2t_{\mathrm{RSA}} + 2H \tag{8}$$

$$E(\delta)=2a+3b+7t_p+t_{2-s}+t_{2-v}+H \quad (9)$$

为了具体分析 DAMIPv6、HAMIPv6 和 2-IBS-HAMIPv6 之间的性能，我们定义模型中的具体参数值：$a=4$ms，$b=2$ms，$t_p=0.5$ms，令 $t_{2-s}=3t_{\mathrm{RSA}}=3t$，$t_{2-v}=5t_{\mathrm{RSA}}=5t$，最后得到三者的数学期望为

$$E(\theta)=56.5+2t+3H \quad (10)$$

$$E(\omega)=49.5+2t+2H \quad (11)$$

$$E(\delta)=17.5+8t+H \quad (12)$$

如图 4 所示，一方面，随着访问域与家乡域之间传输延时的增加，DAMIPv6 的切换延时增长幅度最大，当两地最大传输延时（H 值）达到 40ms 时，DAMIPv6 的切换延时接近 180ms，远远超过其他两种机制. 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，当 H 取最小值 2，签名/验证处理延时达到 10ms 时，2-IBS-HAMIPv6 的切换延时接近 100ms，大于其他两种机制. 在 2-IBS-HAMIPv6 协议中，由于 MN 进入新访问域时，新域必须通过与 MN 家乡域的 HA 交互获得 HA 的 Q_1，增加了与家乡域的交互带来的传输延时. 另外，新域 AR 必须得到 Q_1 后才能对 MN 的签名进行验证，从而降低了协议运行的并发度，增大了切换延时. 在 $t\geq 5.7$ms，$H\leq 28$ms 的部分区域内，HAMIPv6 的切换延时优于 2-IBS-HAMIPv6.

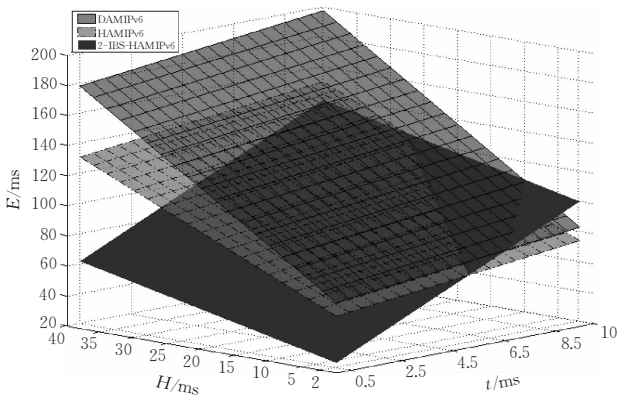


图 4　不同 MAP 域间移动情况下的总切换延时的数学期望

当 MN 在同一 MAP 域内移动时，设新访问域的 NAR 已知 MN 身份 ID 对应的 Q_1 值，MN 已知 MAP_2 身份 ID 对应的 Q_1' 值. DAMIPv6，HAMIPv6 和 2-IBS-HAMIPv6 所需的总切换延时由式(13)～(15)给出：

$$T'_{\mathrm{DAMIPv6}}=6a+8b+6c+21t_p+2t_{\mathrm{RSA}} \quad (13)$$

$$T'_{\mathrm{HAMIPv6}}=4a+8b+4c+17t_p+2t_{\mathrm{RSA}} \quad (14)$$

$$T'_{\text{2-IBS-HAMIPv6}}=2a+4t_p+t_{2-s}+\max(t_{2-v},2b+t_p) \quad (15)$$

当 $a=4$ms，$b=2$ms，$t_p=0.5$ms，令 $t_{2-s}=3t_{\mathrm{RSA}}=3t$，$t_{2-v}=5t_{\mathrm{RSA}}=5t$，最后得到三者的数学期望为

$$E'(\theta)=56.5+2t+3H \quad (16)$$

$$E'(\omega)=44.5+2t+2H \quad (17)$$

$$E'(\delta)=10+8t \quad (18)$$

如图 5 所示，在 2-IBS-HAMIPv6 机制中，一方面，由于 MN 已经在 Q 值列表中建立了 MAP 身份 ID 对应的 Q_1'，因而不再需要 MAP 对 Q_1' 签名并发送给 MN. 另一方面，由于 MAP 域已在 Q 值列表中建立了 MN 父亲身份 ID 对应的 Q_1，因而整个切换认证过程无需与家乡域交互任何信息，大大缩短了总切换延时，且这个值不会随着访问域与家乡域的距离而增长. 而另两种机制则没有明显的改善. 然而，2-IBS-HAMIPv6 机制随着 t 值的增加，切换延时增长幅度仍然很大，在 $t\geq 6.5$ms，$H\leq 12.25$ms 的部分区域内，HAMIPv6 的切换延时仍优于 2-IBS-HAMIPv6.

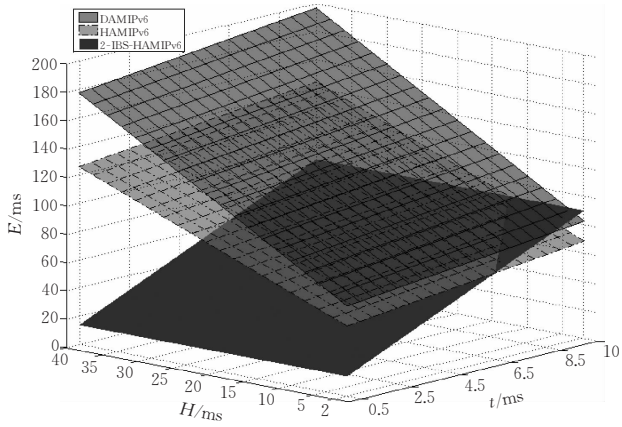


图 5　同一 MAP 域内移动情况下的总切换延时的数学期望

综上所述，当 t 值较高和 H 值较低时，2-IBS-HAMIPv6 机制无法发挥它的优势. 但是，由于 t 值与节点处理能力（CPU 大小，内存大小等）有关，即随着计算机工艺的发展，节点处理能力的增长，t 值必然会不断下降，例如在 Pentium II 233MHz 上进行 1024-b RSA 解密/签名运算所需开销只是 ARM7TDMI 80MHz 上的 1/6[15]. 另外，H 值与访问域和家乡域两地间距离有关，当两地相隔较远时（如图 4 所示的 $H>28$ms，图 5 所示的 $H>12.25$ms），2-IBS-HAMIPv6 机制远好于其他两种. 所以，当网络各实体处理能力较高（在 Pentium III 1GHz 上进行 1024-b RSA 解密/签名运算所需开销低于 10ms①）

① Scott M. Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). Available at http://indigo.ie/~mscott/

且 MN 远离家乡网络,在同一 MAP 域内频繁切换时,2-IBS-HAMIPv6 机制是三者中最优的.

4.2 安全性考虑

我们考虑 4 个安全概念,私钥的保密性、签名的不可伪造性、数据机密性保护和密钥托管,并证明 2-IBS-HAMIPv6 协议满足上述安全性需求.

(1)私钥的保密性.根据 3.1 节设计的签名机制可知,任何第二层用户 $\mathcal{U}$ 的私钥 S_2 都是由它父亲 $\mathcal{P}$ 用私钥 S_1 和随机数 s_1 通过 $S_2=\sum_{i=0}^{1}S_i+s_iP_{i+1}$ 计算得到.虽然 $\mathcal{U}$ 的祖先 $\mathcal{A}$ 生成 $\mathcal{P}$ 的私钥 S_1,但无法获得计算 S_2 时使用的随机数 s_1,因而无法得到 S_2.对于 $\mathcal{P}$ 的其他孩子 $\mathcal{U}'$ 来说,只能获得 S_2' 和 $Q_1=s_1P_0$,另外可从公开参数 *params* 中已知 P_0,但由于计算群 $\mathbb{G}$ 上的 DH 问题是难的,$\mathcal{U}'$ 无法计算出 S_1 和 s_1,也就无法得到 S_2.同理 $\mathcal{P}$ 的兄弟也是无法得到 S_2 的.同理可证明任何第一层 PKGs 的私钥除了其父亲,其他实体也是无法获得的.

所以,任一实体私钥只有它的父亲知道,其他实体包括它的祖先(除了父亲)都无法获得.

(2)签名的不可伪造性.下面先给出一个数学难题的定义.

定义 1. 点加计算 DH 问题(Add-Point Computational Diffie-Hellman Problem,APCDHP).给定 (P,aP,bP,cP,dP),其中 $a,b,c,d\in\mathbb{Z}_q^*$,输出 $acP+bdP$.

定理 1. APCDHP 与 CDHP(Computational Diffie-Hellman Problem)是等效的.

证明. (⇒)假设 APCDHP 是容易的,即给定 (P,aP,bP,cP,dP),能求出 $S=acP+bdP$.那么给定 $(P,a'P,bP,cP,dP)$,就能求出 $S'=a'cP+bdP$.

即可求出 $S-S'=(a-a')cP$.

令 $A=aP$,$A'=a'P$,可以求出 $A-A'=(a-a')P$.因此,该问题就转化为给定 $(P,(a-a')P,cP)$,输出 $(a-a')cP$,即 CDHP.

(⇐)假设 CDHP 是容易的,即给定 (P,aP,cP),能求出 $S=acP$.那么给定 (P,bP,dP),就能求出 $S'=bdP$.

即可求出 $S+S'=acP+bdP$.因此,该问题就转化为给定 (P,aP,bP,cP,dP),输出 $acP+bdP$,即 APCDHP. 证毕.

设用户 $\mathcal{U}$ 的身份是 $ID_{\mathcal{U}}=(I_1,I_2)$,私钥是 $S_{\mathcal{U}}=S_1+s_1P_{\mathcal{U}}$,针对消息 M 的签名 $\langle\sigma\leftarrow S_{\mathcal{U}}+s_2P_M,\ Q_2\leftarrow s_2P_0\rangle$,其中 $P_M=H_1(M,Q_2)$.

考虑敌手 $\mathcal{A}$ 两种不同的伪造签名方式.第一种 $\mathcal{A}$ 通过试图攻破 2-IBS 方案本身达到伪造签名的目的.第二种 $\mathcal{A}$ 通过收集 $\mathcal{U}$ 之前的签名伪装成新的签名进行重放攻击,但由于签名消息中携带了时间戳信息,验证者可以很容易识破这种攻击.

下面证明第一种方式也是不可行的.

本节采用随机预言机模型证明 2-IBS 算法的安全性,即满足适应性选择消息攻击下的不可伪造性.

令敌手 $\mathcal{A}$ 表示一个概率多项式时间的图灵机,输入为 2-IBS 算法的公开参数 $\langle\mathbb{G}_1,\mathbb{G}_2,\hat{e},P_0,Q_0,Q_1,H_1,H_2,p,q\rangle$,其中 $q\geq2^{\ell}$,$\ell=160$.$\mathcal{A}$ 可以向用户 $\mathcal{U}$ 发起 n_1 次签名查询,向随机预言机 H_1 发起 n_2 次查询.

定理 2. 若 $\mathcal{A}$ 可以在时间 t 内以优势 $\varepsilon\geq10(n_1+1)(n_1+n_2)/2^{\ell}$ 产生一个存在性伪造签名,则存在另一个概率算法在时间 $t'\leq120686n_2t/\varepsilon$ 范围内解决 $\mathbb{G}_1$ 群上的 APCDHP.

证明. 根据文献[16-17]中的分叉引理(Forking Lemma),若 $\mathcal{A}$ 可以在时间 t 内以优势 $\varepsilon\geq10(n_1+1)(n_1+n_2)/2^{\ell}$ 产生一个存在性伪造签名,则必然存在另一个概率算法 $\mathcal{B}$,在时间 $t'\leq120686n_2t/\varepsilon$ 范围内产生两个有效签名 (M,Q_2,H_1,σ) 和 (M,Q_2,H_1',σ'),其中 $H_1\neq H_1'$.

基于 $\mathcal{B}$,构造一个概率算法 $\mathcal{C}$.

令算法 $\mathcal{C}$ 的输入为 $\langle P_0,P_1,P_2,Q_0,Q_1\rangle$,其中 $P_1=\alpha P_0$,$P_2=\beta P_0$,$Q_0=s_0P_0$,$Q_1=s_1P_0$.$\mathcal{C}$ 随机选择一个消息 M,运行算法 $\mathcal{B}$,在时间 $t'\leq120686n_2t/\varepsilon$ 范围内得到两个伪造签名 (M,Q_2,H_1,σ) 和 (M,Q_2,H_1',σ'),其中 $H_1\neq H_1'$.有

$$\hat{e}(P_0,\sigma)=\hat{e}(Q_0,Q_2+H_1P_1)\times\hat{e}(Q_1,Q_2+H_1P_2) \tag{19}$$

$$\hat{e}(P_0,\sigma')=\hat{e}(Q_0,Q_2+H_1'P_1)\times\hat{e}(Q_1,Q_2+H_1'P_2) \tag{20}$$

将式(19),(20)两式相除,得

$$\frac{\hat{e}(P_0,\sigma)}{\hat{e}(P_0,\sigma')}=\frac{\hat{e}(Q_0,Q_2+H_1P_1)\times\hat{e}(Q_1,Q_2+H_1P_2)}{\hat{e}(Q_0,Q_2+H_1'P_1)\times\hat{e}(Q_1,Q_2+H_1'P_2)}.$$

$$\hat{e}(P_0,\sigma-\sigma')=\hat{e}(Q_0,(H_1-H_1')P_1)\times\hat{e}(Q_1,(H_1-H_1')P_2),$$

$$\hat{e}(P_0,\sigma-\sigma')=\hat{e}(P_0,(H_1-H_1')S_2),$$

$$\hat{e}(P_0,\sigma-\sigma')\times\hat{e}(P_0,(H_1-H_1')S_2)^{-1}=1.$$

$$\hat{e}(P_0,(\sigma-\sigma')-(H_1-H_1')S_2)=1 \tag{21}$$

令 $(\sigma-\sigma')-(H_1-H_1')S_2=\lambda P_0$,则式(21)得 $\hat{e}(P_0,P_0)^{\lambda}=1$,进而有 $\lambda\equiv0(\bmod q)$.因此,

$$(\sigma-\sigma')-(H_1-H_1')S_2=0(\bmod q),$$

$$S_2=(\sigma-\sigma')(H_1-H_1')^{-1},$$

其中$(H_1-H_1')^{-1}$表示(H_1-H_1')模 q 的乘法逆元.

最终，算法 $\mathcal{C}$ 输出 $S_2=S_1+s_1P_2=s_0P_1+s_1P_2=\alpha s_0P_0+\beta s_1P_0$. 根据之前的定义 1，$\mathbb{G}_1$ 群上的 APCDHP 就是给定(P,aP,bP,cP,dP)，其中 $a,b,c,d\in\mathbb{Z}_q^*$，输出 $acP+bdP$. 这就意味着算法 $\mathcal{C}$ 在给定输入$\langle P_0,\alpha P_0,\beta P_0,s_0P_0,s_1P_0\rangle$的情况下，输出了 $\alpha s_0P_0+\beta s_1P_0$，即在时间 $t'\leq 120686n_2t/\varepsilon$ 范围内解决了 $\mathbb{G}_1$ 群上的 APCDHP. 证毕.

(3) 数据的机密性保护. 在传统的无线移动环境中，移动协议消息和认证消息的传输都是承载在事先建立好的安全关联(SA)之上，受安全关联的保护. 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都需要建立一对 SA，如 MAP 与 AAAv 之间、AAAv 与 AAAh 之间、AAAh 与 HA 之间等等，SA 的建立与维护给网络和各节点带来沉重的负担. 根据基于身份密码学的特点，可以很容易解决这个问题. 在 2-IBS-HAMIPv6 机制中，消息发送方使用接受方的身份 ID 对消息加密，只有拥有该 ID 对应私钥的接受方才能对加密消息进行解密，从而实现数据的机密性保护. 这种方式取消了 SA 的建立，并可在任何时候与任何人建立一条安全的传输通道，而具体加密算法的实现则可参考文献[8].

(4) 密钥托管. 由于实体私钥是由它的父亲计算生成，因而其父亲可以伪造该实体签名或监听该实体加密通信. 但是，由于实体私钥只和其父亲有关，任何其他实体均无法获得其私钥. 因而在无线移动环境中，实体离开家乡域后，进入任何本地域时，任何节点包括本地域的 MAP 都无法假冒该实体行为或监听该实体的加密通信. 因而可以说在一个独立的外地域环境中，2-IBS-HAMIPv6 机制有效消除了密钥托管带来的危害. 另外，若第二层实体事先以某种形式公开 Q_2，即明确该实体使用的 s_2，则它的父亲将无法伪造 Q_2 和 s_2，也就无法伪造该实体的签名或监听该实体的加密传输信道.

4.3　可扩展性考虑

由于 HMIPv6 协议并没有推荐 MAP 的最优层次数，为了简便，本文实现了一种 2 层身份认证机制. 由于多级 MAP 是可能存在的，因而本文提出的机制应该能够支持多级 MAP 的情况. 2-IBS-HAMIPv6 很容易扩展为多层机制，如图 6 所示. 具体描述如下：

同一根 PKG 域内所有实体均可获得系统公开参数 $params$，因此域内任意两个实体间只需要知道

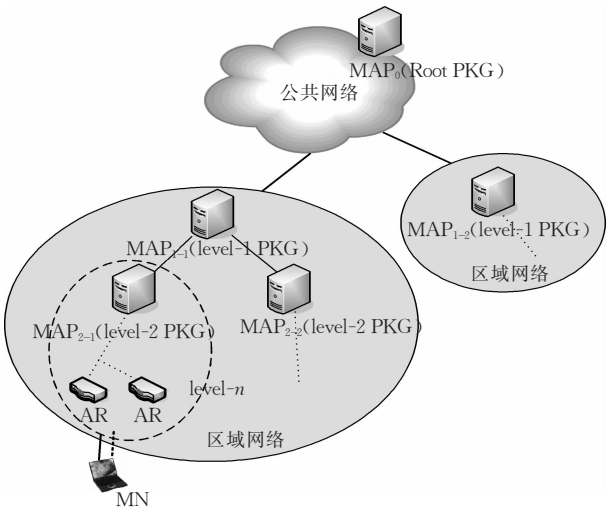


图 6　层次化接入认证机制的扩展

对方身份 ID 对应 Q 值就可实现签名/验证过程. 设 MN 的身份 $ID_{MN}=(I_1,\cdots,I_k,I_{k+1},\cdots,I_m)$，AR 的身份 $ID_{AR}=(I_1,\cdots,I_k,I'_{k+1},\cdots,I'_n)$，两者拥有共同的身份前缀$(I_1,\cdots,I_k)$，当 AR 需要验证 MN 的签名时，AR 需要向上层 PKG 递归查询$(I_{k+1},\cdots,I_m)$对应的所有 Q 值，并建立相应 Q 值列表. 反之则需要$(I'_{k+1},\cdots,I'_n)$对应的各层 PKG 将相应 Q 值签名通过 AR 转发给 MN. 随着层数的增加，查询 Q 值所需的交互次数将线性增长，切换延时也将显著增长. 但是，若 MN 的身份 ID 对应 Q 值列表已经建立，即 MN 在某个 MAP 域内频繁移动时，根据公式(18)所示，2-IBS-HAMIPv6 的切换延时将大幅度下降. 不过，随着层数的增加，签名的长度和签名/验证算法的处理延时也将线性增长.

5　结束语

本文提出了一种基于身份签名的层次化认证机制，该机制通过采用 HIBS 技术替代了传统的基于公钥证书的方式，实现了移动 IPv6 网络中安全、高效的网络与用户的双向认证. 通过采用分级的身份标识作为每个节点的公钥，大大降低了管理密钥给每个节点带来的负担. 与传统基于公钥证书的方式比较，本文提出的方法消除了移动节点为请求或维护证书带来的沉重的操作或通信负担. 另外，该机制利用层次化基于身份签名方案的特性，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消息交互. 性能分析表明当移动节点远离家乡和节点处理能力不断提升时，我

们的方案远好于其他方案.

本文提出的方案集中在移动 IPv6 场景,虽然实现的是一个 2 层结构的接入认证框架,但能很容易扩展到支持多层结构.不过本文实现的层次化签名机制会随着层次数的增长,签名长度和签名/验证效率会线性增长.因此可以参考文献[11]设计的固定密文、固定解密开销的 HIBE 机制,实现一种类似的 HIBS 机制.另外本文虽然只实现了接入认证,但可很容易基于 IBE 实现数据的机密性保护.同时,本文提出的方案部分解决了密钥托管问题,但仍然存在父亲知道孩子私钥的情况,因此还有必要设计一种完全解决密钥托管问题的机制.若要解决上述三个问题,同样会带来新的计算开销,如何降低这些开销将是我们下一步工作的重点.

参 考 文 献

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

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

[3] Gergiades M, Akhtar N, Politis C et al. AAA context transfer for seamless and secure multimedia services over All-IP infrastructures//Proceedings of the 5th European Wireless Conference (EW'04). Barcelona, 2004: 442-448

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

[5] Aboba B, Simon D. PPP EAP TLS authentication protocol. RFC 2716, October, 1999

[6] Lee B G, Kim H G, Sohn S W et al. Concatenated wireless roaming security association and authentication protocol using ID-based cryptography//Proceedings of the IEEE Vehicular Technology Conference (VTC'03). Spring, Jeju, 2003, 3: 1507-1511

[7] Shamir A. Identity-base cryptosystems and signature schemes//Advances in Cryptology-Crypto'84. LNCS 196. Heidelberg: Springer-Verlag, 1984: 47-53

[8] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. SIAM Journal of Computing, 2003, 32(3): 586-615

[9] Horwitz J, Lynn B. Toward hierarchical identity-based encryption//Advances in Cryptology-Eurocrypt'02. LNCS 2332. Heidelberg: Springer-Verlag, 2002: 466-481

[10] Gentry C, Silverberg A. Hierarchical ID-based cryptography//Advances in Cryptology-Aisacrypt'02. LNCS 2501. Heidelberg: Springer-Verlag, 2002: 548-566

[11] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext//Advances in Cryptology-Eurocrypt'05. LNCS 3494. Heidelberg: Springer-Verlag, 2005: 440-456

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

[13] Tian Ye, Zhang Yu-Jun, Liu Ying, Li Zhong-Cheng. A fast authentication mechanism using identity based signature in mobile IPv6 network. Journal of Software, 2006, 17(9): 1800-1888(in Chinese)
(田 野,张玉军,刘 莹,李忠诚. 移动 IPv6 网络基于身份签名的快速认证方法. 软件学报, 2006, 17(9): 1800-1888)

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

[15] Galbraith S, Harrison K, Soldera D. Implementing the Tate pairing//Proceedings of the Algorithm Number Theory Symposium (ANTS V). LNCS 2369. Heidelberg: Springer-Verlag, 2002: 324-337

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

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

TIAN Ye, born in 1979, Ph. D.. His research interests include the next generation networks and the wireless mobile network security.

ZHANG Yu-Jun, born in 1976, Ph. D., associate professor. His research interests include the next generation networks and mobility computing.

ZHANG Han-Wen, born in 1981, Ph. D. candidate. Her research interests include the next generation Internet and the wireless mobile network.

LI Zhong-Cheng, born in 1962, Ph. D., professor. His research interests include computer networks and trusted computing.

Background

Two issues should be considered for deploying mobile IPv6 networks. The first one, the users who want to access networks should be authenticated. This process is called access authentication. The second one, handover performance integrating authentication should be improved possibly. Handover and authentication usually occur at the same time. Authentication procedure may affect handover performance inevitably, such as increasing handover latency. In this paper, we focus on minimizing handover latency integrating authentication.

All of the current solutions for the authentication in the wireless mobile environment only append authentication procedure into the handover procedure, but don′t specify authentication method. But what affects handover performance mostly is authentication method. Currently the mostly mutual authentication methods are based on the public key infrastructure (PKI). But in wireless mobile networks, terminal users can′t know the access network certificate authority address, and then can′t obtain certificates. PKI-based authentication methods may not be suitable to wireless mobile networks. In addition, some authors proposed an AAA (Authentication, Authorization and Accounting) authentication protocol based on identity based cryptography, which could be used in the mobile IPv4 and WLAN environment. It used NAI, which was the form like username@homedomain, as the public key to simplify key management. This solution avoided the problems arose by PKI-based authentication methods, but didn′t optimize handover performance integrating authentication, which is the key issue in the wireless mobile environment.

In this paper, the authors design a two-level hierarchical identity based signature (2-HIBS) scheme, based on which the authors propose a new hierarchical authentication scheme for wireless mobile IPv6 networks. The solution can achieve higher handover performance by the simpleness of HIBS and hierarchical handover scheme. And its security is built on the difficulty of the computational Diffie-Hellman problem (CDHP).

This research work was established in the Institute of Computing Technology, Chinese Academy of Sciences in 2005. It was supported by the National Natural Science Foundation of China (90604014). The NSF project wants to solve the key issues in the wireless mobile environment integrating access control, which includes the framework of the wireless mobile networks integrating access control, the mutual authentication methods for the wireless mobile environment, the hierarchical region registration schemes. The research work of this paper belongs to the mutual authentication methods for the wireless mobile environment. In this aspect, the authors have published two papers, one is "A fast authentication mechanism using identity based signature in mobile IPv6 network" in Journal of Software, and another is "A Survey of Identity-Based Cryptography using Pairing" in Journal of Computer Research and Development.