软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(9):2465−2480 [doi: 10.3724/SP.J.1001.2012.04188]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

节点证书与身份相结合的 HMIPv6 网络接入认证机制*

高天寒[1], 郭 楠[2+], 朱志良[1]

[1](东北大学 软件学院,辽宁 沈阳 110006)

[2](东北大学 信息科学与工程学院,辽宁 沈阳 110006)

Access Authentication for HMIPv6 with Node Certificate and Identity-Based Hybrid Scheme

GAO Tian-Han[1], GUO Nan[2+], ZHU Zhi-Liang[1]

[1](Software College, Northeastern University, Shenyang 110006, China)

[2](College of information Science and Engineering, Northeastern University, Shenyang 110006, China)

+ Corresponding author: E-mail: Gaonan@mail.neu.edu.cn

Gao TH, Guo N, Zhu ZL. Access authentication for HMIPv6 with node certificate and identity-based hybrid scheme. *Journal of Software*, 2012,23(9):2465−2480 (in Chinese). http://www.jos.org.cn/1000-9825/4188.htm

Abstract: Access authentication is the basic security requirement of hierarchical mobile IPv6 (HMIPv6) network. A mutual access authentication scheme is proposed in this paper based on hierarchical authentication framework as well as node certificate and identity-based hybrid approach. The scheme adopts identity-based cryptography to simplify the cumbersome key management of PKI. Node certificate is introduced to authenticate entity, which eliminates message interactions between home network and access network. A mutual authentication protocol is achieved using proposed hierarchical signature mechanism. The protocol can also be extended to support access authentication in multi-level HMIPv6 network. Performance and security analysis demonstrates that the proposed scheme outperforms other identity-based proposals in terms of efficiency and security.

Key words: mobile IPv6; hierarchical mobile IPv6; mutual access authentication; identity-based signature; node certificate

摘 要: 接入认证是层次型移动 IPv6(HMIPv6)网络安全的基本需求.构建了适于 HMIPv6 的分层认证框架,设计了一种节点证书与身份相结合的签名方案,并以此为基础提出了 HMIPv6 网络双向接入认证机制.该机制利用基于身份密码技术简化了公钥基础设施的复杂密钥管理过程;以节点证书为接入认证的主要依据,消除了接入网络与家乡网络间的消息交互;采用提出的层次化签名方案,实现了用户与接入网络的双向认证.机制经过简单扩展,能够支持多层 HMIPv6 网络的接入认证.性能与安全性分析表明,与传统的及其他基于身份的认证方案比较,所提出的机制拥有更高的认证效率和安全性.

关键词: 移动 IPv6;层次型移动 IPv6;双向接入认证;身份签名;节点证书

中图法分类号: TP393 **文献标识码**: A

随着移动设备数量和接入网络需求的不断增加,互联网正向支持大范围移动性方向发展,移动 IPv6

* 基金项目: 国家自然科学基金(60872040); 中央高校基本科研业务费专项资金(N100417002, N100404004)
收稿时间: 2011-07-14; 修改时间: 2011-09-02; 定稿时间: 2012-01-16

(MIPv6[1])将成为下一代移动通信的重要支撑协议.为进一步提升 MIPv6 的适用性以及移动节点在外地网络中的切换效率,IETF 对 MIPv6 进行了扩展,制定了层次型移动 IPv6 协议(HMIPv6)[2],在外地网络中引入移动锚点对移动节点实施区域化移动管理,以降低移动节点切换延时,但缺乏安全性方面的考虑.移动互联网的开放性增加了潜在安全威胁,当移动节点接入外地网络时,需要同外地网络相互认证身份,这是安全通信的基本需求.另外,移动节点的切换和认证往往同时发生,为保障实时应用,认证机制应与切换过程同步进行,尽可能保证切换效率.针对 HMIPv6 的高效双向接入认证机制成为研究热点.

基于 PKI(public key infrastructure)[3]和 AAA(authentication, authorization and accounting)[4]可以实现节点间的身份认证,而传统的 PKI 和 AAA 主要是针对有线网络环境提出的认证框架,没有考虑接入方式不同及网络拓扑结构动态变化所带来的差异.现有研究结合 MIPv6 和 HMIPv6 对 PKI 及 AAA 框架进行改进,解决移动节点与接入网络间的身份认证问题.基于 PKI 的解决方案包括:IETF 推荐使用 IPSec[5]保护 MIPv6 和 HMIPv6 的移动管理消息,并实现节点间的身份认证.IPSec 利用 IKE 协议[6]建立节点间的安全关联,并利用 PKI 确保此过程的安全.建立安全关联的节点通过认证扩展包头进行双向身份认证;文献[7]构建了面向 HMIPv6 的 PKI 认证框架,对 IKE 协议进行修改,基于节点所属认证中心(CA)间的信任关系以及新的可信数字证书仓库,实现移动节点与移动锚点间的双向认证;文献[8]对返回路由可达过程[1]进行修改,实现 MIPv6 下移动节点与通信伙伴间的安全路由优化、双向身份认证和会话密钥协商,移动节点以家乡代理颁发的证书作为对其认证的主要凭证,整个机制依赖于 PKI 在实体间传递信任.面向 AAA 的解决方案包括:文献[9]将 AAA 框架移植到移动网络环境中,在 MIPv6 或 HMIPv6 中部署 AAA 实体,利用 Diameter 协议[10−12]承载认证消息,通过家乡网络和接入网络的消息传递,最终实现移动节点与接入网络间的身份认证;为提高移动节点切换效率,文献[13]将认证消息与 HMIPv6 移动注册消息紧密结合,基于挑战/应答方式和移动节点与家乡代理间的一次消息往返,完成移动注册和节点认证;文献[14]提出了适于 HMIPv6 的层次化 AAA 框架,利用建立短期外地关联和上下文转移技术提高系统性能.

上述基于 PKI 或 AAA 的接入认证机制均利用普遍存在的基础设施或预先签订好的漫游约定建立家乡网络和接入网络间的信任关系,在网络结构动态变化的移动环境中,部署和实施起来比较困难.信任域间的消息传递和认证消息处理给移动节点带来切换延时,影响实时网络应用.另外,对 PKI 中的公钥证书维护及 AAA 框架下复杂认证协议的支持,将给计算能力较弱的移动节点带来沉重负担,无法实现高效接入认证.

近年来,研究者将基于身份的密码学应用于移动网络接入认证过程[15−19],旨在消除对 PKI 和 AAA 框架的依赖.文献[15]是对 HMIPv6 在安全性方面的改进协议,采用 SEND 协议[20]中的加密生成地址(CGA[21])技术实现跨信任域的接入认证.加密生成地址中包含节点的公钥信息,能够有效防止 IP 地址欺骗等攻击,不需要附加 PKI 等安全设施.然而由于加密生成地址持有者的真实身份没有办法被认证,恶意节点可以产生合法的加密生成地址而接入网络.文献[16]设计了基于快速分层移动 IPv6[22]的安全网络架构,采用全新的地址构造方式将节点身份信息附加在 IP 地址中,运用身份密码学解决了移动环境中的接入认证、安全路由优化和会话密钥分配等问题,但特殊的 IP 地址生成和管理方式使该机制缺乏广泛适用性.文献[17]设计了基于身份的层次化签名方案,将分级网络访问标识符(NAI)作为公钥,简化无线环境中的密钥管理,实现了 HMIPv6 下移动节点与接入网络的双向认证.同时,将层次化移动管理过程同认证过程有机整合,减少了家乡网络和接入网络间的消息交互,提升了移动节点的切换效率.然而,该方案仍然没有摆脱家乡网络和接入网络预先信任的安全假设,家乡代理仍需要参与认证过程,在一定程度上限制了方案的高效性.

本文设计了一种节点证书与身份相结合的签名方案,并以此为基础提出了 HMIPv6 网络双向接入认证机制.该机制以全新定义的节点证书作为接入认证的主要依据,消除了接入网络与家乡网络间的消息交互,提高了认证效率和灵活性.同时,该机制仅作域内可信假设,家乡网络和接入网络可以不存在预先的信任关系,增强了机制的适用性.性能与安全性分析表明,本文提出的机制同传统的及其他基于身份的认证方案相比较,拥有更高的认证效率和安全性.

本文第 1 节简要介绍层次型移动 IPv6 协议和基于身份的签名技术.第 2 节给出节点证书定义,设计证书与身份相结合的签名方案,并重点描述基于此方案的双向接入认证实现过程.第 3 节给出安全性分析和性能分析.

第 4 节总结全文.

1 相关背景

1.1 层次型移动IPv6协议

HMIPv6 在外地网络中设置移动锚点(MAP)对移动节点实施区域化移动管理.MAP 管辖若干接入路由器,构成 MAP 域.MAP 定期向域内接入路由器发送 MAP 选项,维护 MAP 的最新状态.当移动节点进入 MAP 域后,首先接收到接入路由器广播的路由器公告消息,移动节点根据此公告消息配置本地关照地址和域内关照地址.随后,移动节点向 MAP 发送域内绑定更新消息进行域内注册,通知本地关照地址和域内关照地址的绑定关系.同时,移动节点向家乡代理发送远程绑定更新消息进行家乡注册,通告其在外地网络所获得的域内关照地址.此后,家乡代理将发往移动节点的数据包通过隧道封装的方式发送至移动节点的域内关照地址,MAP 截获数据包并最终将其转发至移动节点的本地关照地址.当移动节点在 MAP 域内的不同接入路由器间切换时,只需向 MAP 发送域内绑定更新消息,通知其在新接入路由器处获得的新的本地关照地址,而保持域内关照地址不变.移动节点不再向家乡代理发送远程绑定更新消息,仅当移动节点产生跨 MAP 域移动时才重新进行家乡注册.移动节点在外地网络的移动管理操作和移动管理消息均局限在 MAP 域内.

当移动节点在外地网络频繁移动时,HMIPv6 能够显著提升移动节点切换效率.然而,HMIPv6 在设计时没有考虑移动管理过程中的安全性问题.移动节点进入 MAP 域后,如果不对其接入过程进行控制,可能会产生大量的安全威胁,遭受非法访问、拒绝服务(DoS)和重定向等攻击.而安全防护的重要基础是身份认证.首先,MAP 及接入路由器应能对移动节点的合法身份进行认证,防止恶意节点对接入网络资源的非法访问和使用;其次,移动节点同样需要验证 MAP 和接入路由器的合法身份,避免中间人攻击等威胁给正常通信带来的影响.从保障网络安全可靠运营的角度,移动节点与接入网络必须实施双向身份认证.另外,如果对移动节点的身份认证和移动管理操作分离实施,将给移动节点带来切换延时,影响实时网络应用.因此,应尽可能将双向接入认证与移动管理过程有机整合,提出高效的认证机制.

1.2 基于身份的签名技术

对基于身份签名技术的研究始于 Shamir 在 1984 年提出的基于身份密码学(IBC)[23].在基于身份签名中,用户公钥可以是与用户任意身份信息关联的二进制比特流,而且设置了一个可信的授权机构(PKG)负责公共参数的生成并根据身份信息为用户分配对应私钥.基于身份签名的最大优势在于简化了传统 PKI 下复杂的数字证书管理和维护过程,验证方只需要知道签名方的公开身份信息及一些系统参数就可以完成对签名的验证.然而,基于身份密码学诞生后所提出的一系列基于身份签名方法的安全性都没有经过严格证明.直到 2001 年,Boenh 和 Franklin 应用双线性对技术构建了第一个安全且实用的基于身份的公钥密码体制[24].此后,大量使用双线性对的基于身份签名方案被提出并被应用到不同领域.

1.2.1 双线性对(bilinear pairing)

令 G 和 G_T 分别是阶为大素数 q 的加法群和乘法群,I_G 为 G 的生成元,I_{G_T} 为 G_T 的生成元.$\hat{e}:G\times G\to G_T$ 是一个映射,如果 $\hat{e}$ 具备以下特性,则称 $\hat{e}$ 是一个双线性对.

(1) 双线性:对于所有的 $P,Q\in G$ 及 $a,b\in Z_q^*$,满足 $\hat{e}(aP,bQ)=\hat{e}(bP,aQ)=\hat{e}(P,Q)^{ab}$,其中,$Z_q^*=\{1,2,...,q-1\}$;

(2) 非退化性:存在 $P,Q\in G$,使得 $\hat{e}(P,Q)\neq I_{G_T}$;

(3) 可计算性:对于所有的 $P,Q\in G$,存在有效计算 $\hat{e}(P,Q)\in G_T$.

在密码学中,可以利用双线性对构造很多其他数学工具所无法实现的安全方法.超奇异椭圆曲线上的 Weil 对和 Tate 对[25]就是两个典型的双线性对,而现有的基于身份签名机制大多是基于这两种方法构建的.

1.2.2 基于身份签名机制

基于身份签名(IBS)机制通常包括 4 种算法:参数生成算法(Setup)、密钥分配算法(Extract)、签名算法(Sign)和验证算法(Verify).Setup 和 Extract 由 PKG 执行,生成系统参数和主密钥,同时为用户分配与身份信息对应的私

钥.签名方使用私钥和 Sign 对消息签名,验证方通过用户公开的身份信息生成公钥并使用 Verify 对签名进行验证.下面通过高效、安全的 Hess 签名[26]描述 IBS 的工作过程:

- Hess-IBS_Setup:*PKG* 选择加法群 G_1、乘法群 G_2 及双线性对 $\hat{e}:G_1\times G_1\to G_2$;*PKG* 选择 $s\in Z_q^*$ 作为主密钥,计算 $P_{pub}=sP$ 作为系统公钥,$P\in G_1$;*PKG* 定义哈希函数 $H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\times G_2\to Z_q^*$;*PKG* 公开系统参数 Params: $\langle G_1,G_2,\hat{e},P,P_{pub},H_1,H_2\rangle$;
- Hess-IBS_Extract:签名方将身份 ID 发送给 *PKG*,*PKG* 生成并分配用户私钥 $S_{ID}=sQ_{ID}$,$Q_{ID}=H_1(ID)$;
- Hess-IBS_Sign:为对消息 m 签名,随机选择 $P_1\in G_1,k\in Z_q^*$,计算:

  (a) $r=\hat{e}(P_1,P)^k$;

  (b) $v=H_2(m,r)$;

  (c) $u=vS_{ID}+kP_1$.

  签名结果为 $\sigma=(u,v)\in G_1\times Z_q^*$;
- Hess-IBS_Verify:验证方已知消息 m 和签名 σ,计算 $r'=\hat{e}(u,P)\cdot\hat{e}(Q_{ID},-P_{pub})^v$,若 $v==H_2(m,r')$则接受签名,否则拒绝.

1.2.3 层次型基于身份签名机制

为减轻 IBS 中 PKG 的负担并增强 IBS 的可扩展性,文献[27]提出了层次型基于身份签名机制(HIBS),设置多个 PKG 形成层次化结构,用户身份由一个多元组表示($ID_1,ID_2,\ldots,ID_t$).HIBS 包括 5 种算法:*Root-setup*,*Lower-level-setup*,*Extract*,*Sign* 和 *Verify*.*Root-setup* 和 *Lower-level-setup* 分别由根 PKG(root PKG)和低层 PKG 执行.HIBS 具体工作过程如下:

- HIBS_Root-setup:root PKG 选择加法群 G_1、乘法群 G_2 及双线性对 $\hat{e}:G_1\times G_1\to G_2$;*root PKG* 选择 $s_0\in Z_q^*$ 作为主密钥,计算 $Q_0=s_0P_0$ 作为系统公钥,$P_0\in G_1$;root PKG 定义哈希函数 $H_1:\{0,1\}^*\to G_1$,$H_2:\{0,1\}^*\to G_1$;*root PKG* 公开系统参数 Params: $\langle G_1,G_2,\hat{e},P_0,Q_0,H_1,H_2\rangle$;
- HIBS_Lower-level-setup:下层 *PKG* 随机选择 S_t,秘密保存;
- HIBS_Extract:下层 *PKG* 或用户(E_t)的密钥由上层 *PKG*(PKG_{t-1})计算和分配:

  (a) $P_t=H_1(ID_1,\ldots,ID_t)$;

  (b) 计算 E_t 私钥 $S_t=S_{t-1}+s_{t-1}P_t=\sum_{i=1}^{t}s_{i-1}P_i$;

  (c) 给 E_t 分配 $Q_i=s_iP_0$,$1\leqslant i\leqslant t-1$.
- HIBS_Sign:签名方($ID_1,\ldots,ID_t$)使用私钥 S_t 对消息 m 签名:

  (a) $P_m=H_1(ID_1,\ldots,ID_t,m)$;

  (b) $\sigma=S_t+s_tP_m$.

  签名方发送{$ID,\sigma,Q_i(1\leqslant i\leqslant t)$}给验证方;
- HIBS_Verify:验证方验证等式 $\hat{e}(P_0,\sigma)==\hat{e}(Q_0,P_1)\cdot\hat{e}(Q_t,P_m)\cdot\prod_{i=2}^{t}\hat{e}(Q_{i-1},P_i)$.若等式成立则接受签名,否则拒绝.

2 节点证书与身份签名相结合的双向接入认证机制

现有的基于身份的 HMIPv6 接入认证方案虽然摆脱了对 PKI 和 AAA 的依赖,但仍然需要建立家乡网络和接入网络预先信任的安全假设,不具有普遍适用性.另外,家乡代理(HA)参与认证过程,MAP 与 HA 需要交互认证消息,而且认证与移动管理缺乏并行组织,这些都限制了方案的高效性.更重要的是,HA 缺乏对移动节点(MN)的有效控制,认证过程中的相关信息(节点身份、Q 值等)没有得到保护,影响了方案的安全性.本节设计基于节点证书的 HIBS 机制,构建层次化认证框架,实现 HMIPv6 中用户与接入网络的高效双向接入认证.

2.1 基于节点证书的HIBS机制

为保护认证信息并提高认证效率和灵活性,引入节点证书概念.这里的节点证书不同于 PKI 体系下的数字证书,将在认证过程中发挥重要作用.

定义 1(**节点证书**(**node certificate**)). 实体 E_t 的节点证书(简称证书,记为 $Cert\_E_t$)由上层 *PKG* 颁发,包括 Q 值集合($Q_1,Q_2\ldots,Q_t$)、E_t 的身份($ID_1,ID_2\ldots,ID_t$)、节点类型(Type)和上层 *PKG* 的签名(σ_{PKG}).其中,节点类型具体分为:*PKG*、固定节点(FN)和移动节点(MN).

对 HIBS 进行改进,设计了基于证书的 HIBS 机制(C-HIBS),包括 5 个算法:Root-setup,Lower-level-setup,Extract-cert-gen,Sign 和 Verify,具体工作过程如下:

- C-HIBS_Root-setup:root PKG 选择加法群 G_1、乘法群 G_2 及双线性对 $\hat{e}:G_1\times G_1\to G_2$;root PKG 选择 $s_0\in Z_q^*$ 作为主密钥,计算 $Q_0=s_0P_0$ 作为系统公钥,$P_0\in G_1$;root PKG 定义哈希函数 $H_1:\{0,1\}^*\to G_1,H_2:\{0,1\}^*\to G_1,H_3:\{0,1\}^*\times G_2\to Z_q^*$;root PKG 公开系统参数 Params: $\langle G_1,G_2,\hat{e},P_0,Q_0,H_1,H_2,H_3\rangle$;
- C-HIBS_Lower-level-setup:下层 PKG 或用户(E_t)随机选择 S_t 秘密保存,并计算:
  (a) $P_{t-1}=H_1(ID_1,\ldots,ID_{t-1})$;
  (b) $Q_t=s_tP_{t-1}$.
- C-HIBS_Extract-cert-gen:E_t 发送 ID_{E_t},Q_t 给 PKG_{t-1},PKG_{t-1} 计算:
  (a) $P_t=H_1(ID_1,\ldots,ID_t)$;
  (b) E_t 私钥 $S_t=S_{t-1}+s_{t-1}P_t=\sum_{i=1}^{t}s_{i-1}P_i$;
  (c) 用 *Hess-IBS* 对 $(Q_1,\ldots,Q_t,ID_{E_t},Type)$ 签名,结果为 $\sigma_{PKG_{t-1}}$;
  (d) 生成 $Cert\_E_t$,包括 $(Q_1,\ldots,Q_t,ID_{E_t},Type,\sigma_{PKG_{t-1}})$.
  PKG_{t-1} 返回 $S_t,Cert\_E_t$ 给 E_t;
- C-HIBS_Sign:签名方($Signer_t$)使用私钥 S_t 对消息 m 签名:
  (a) $P_m=H_1(ID_1,\ldots,ID_t,m)$;
  (b) $\sigma=S_t+s_tP_m$.
  签名方发送 ID_{Signer_t},σ,$Cert\_Signer_t$ 给验证方;
- C-HIBS_Verify:验证方首先用 Hess-IBS 验证 $Cert\_Signer_t$ 中的σ;若成功,从 $Cert\_Signer_t$ 中提取 $Q_i(1\leqslant i\leqslant t)$和 ID_{Signer_t},继续验证等式 $(P_0,\sigma)==\hat{e}(Q_0,P_1)\cdot\hat{e}(Q_t,P_m)\cdot\prod_{i=2}^{t}\hat{e}(Q_{i-1},P_i)$;若等式成立则接受签名,否则拒绝.

2.2 面向域的二层认证框架

为适应 HMIPv6 的网络结构,构建了二层认证框架.如图 1 所示,框架由一个根 PKG(root PKG)、若干一层 PKG 和二层用户组成.一层 PKG 包括 HA 和 MAP,二层用户包括 MN、接入路由器(AR)及固定节点(FN).根据一层 PKG 的管辖区域把框架划分成若干管理域,HA 所在的家乡网络为家乡域,MAP 所处的外地网络构成 MAP 域,一层 PKG 为域管理者.根 PKG 生成系统参数,并根据身份信息为一层 PKG 分配私钥并颁发证书;一层 PKG 作为域管理者不但负责域内节点的移动管理,还根据身份信息和节点类型为域内二层用户分配私钥、颁发证书.对框架内的功能实体作如下约定和设置:

(1) 仅作域内可信假设.只有管理域内的节点(如 HA 和 MN)间可信并存在预设安全信道,除根 PKG 和一层 PKG 外,任何域间节点(如 MAP 和 HA)不存在预设安全信道;
(2) 可信节点间预先共享对称密钥,可以用 HMAC 机制[28]对传输的消息进行保护;
(3) 采用分级网络访问标识符(NAI)[18]标识节点身份.如,一层 PKG 身份为 Domain.net,二层用户身份为 User@Domain.net;
(4) PKG 支持 Hess-IBS 和 HMAC,二层用户支持 Hess-IBS,C-HIBS 和 HMAC;
(5) 所有节点均维护一张证书列表(CL),用于存储自身和其他相关节点的证书;

(6) 为抵抗重放攻击,签名消息须携带时间戳.

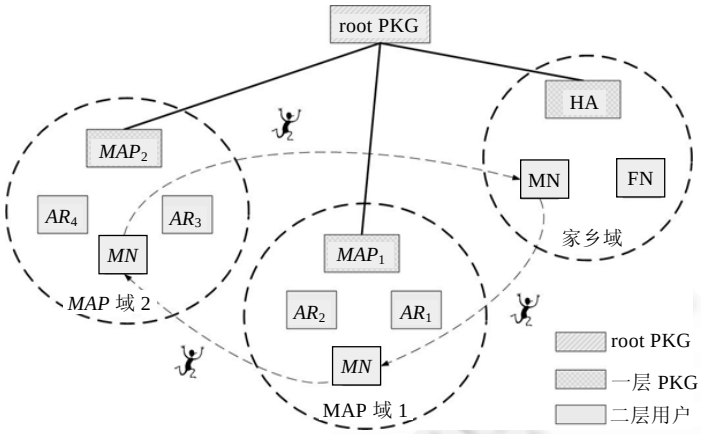

Fig.1 2-Level authentication framework

图 1 二层认证框架

框架下相关操作的标识及说明见表 1.

Table 1 Notations and explanations

表 1 标识及说明

标识	说明
$A\rightarrow B:[M]$	实体 A 通过非安全信道发送消息 M 给实体 B
$A\sim B:[M]$	实体 A 通过安全信道发送消息 M 给实体 B
$Cert\_A$	实体 A 的证书
σ	数字签名,简称签名
$\{M\}_{\alpha\_Sign\_Signer}$	签名方(Signer)使用算法α对消息 M 签名
$\{M,\sigma\}_{\beta\_Verify\_Verifier}$	验证方(Verifier)使用算法β对消息 M 的签名进行验证
$K_{A\text{-}B}$	实体 A 和 B 共享的对称密钥
$(M)_{MAC}$	HMAC 机制中消息 M 的认证码,$(M)_{MAC}=HMAC(K_{A\text{-}B},M)$
TS	时间戳

2.3 双向接入认证协议

基于 C-HIBS 和二层认证框架,设计了 HMIPv6 双向接入认证协议.结合 MN 的移动过程(如图 1 所示)描述协议的具体实现.

(1) MN 处于家乡域

MN 移动前,假设二层认证框架下的各功能实体已基于 C-HIBS 完成 Root-setup,Lower-level-setup 和 Extract-cert-gen 操作,即所有系统参数配置完毕,且实体均已获得相应私钥和证书.

(2) MN 进入 MAP 域

如图 2 所示,MN 接入 MAP_1 域中的 AR_1,并接收到 AR_1 的路由器通告(RA),此通告携带 AR_1 的证书.

① $AR_1\rightarrow MN:[RA,Cert\_AR_1]$:

1) MN 首先开始移动注册.为保护注册消息,MN 分别对远程绑定更新消息(RBU)和域内绑定更新消息(LBU)进行 HMAC 保护和 C-HIBS 签名;
2) MN 随后验证 $Cert\_AR_1$:$\{Cert\_AR_1\}_{Hess\text{-}IBS\_Verify\_MN}$,如果成功,则 MN 从 $Cert\_AR_1$ 中提取 ID_{AR_1} 及 Q 值集合 (Q_{MAP_1},Q_{AR_1});

② $MN\rightarrow AR_1:[RBU,LBU,TS_1,(RBU)_{MAC}=HMAC(K_{MN\text{-}HA},RBU,TS_1),\sigma_1=\{LBU,TS_1\}_{C\text{-}HIBS\_Sign\_MN},Cert\_MN]$:

AR_1 首先检查 TS_1 的新鲜性,然后检查证书列表(CL),由于 MN 初次接入 AR_1,因此 CL 中没有 $Cert\_MN$

表项.AR_1 向 MAP 发送证书认证请求消息(CVR),请求对 *Cert_MN* 进行认证;

③ AR_1~MAP_1:[*CVR*,*RBU*,$(RBU)_{MAC}$,TS_1,*LBU*,*Cert_MN*]:

1) MAP_1 验证 $Cert\_MN:\{Cert\_MN\}_{Hess\text{-}IBS\_Verify\_MAP_1}$,如果成功,则 MAP_1 检查 MN 的节点类型,如果为移动节点,则根据 LBU 临时更新绑定缓存;

2) MAP_1 向 AR_1 回送证书认证确认消息(CVA)和域内绑定确认消息(LBA);

3) MAP_1 向 HA 转发 MN 的 RBU;

④a MAP_1~AR_1:[*CVA*,*LBA*]:

1) 收到 CVA 后,AR_1 从 *Cert_MN* 中提取 ID_{MN} 和 *Q* 值集合(Q_{HA},Q_{MN}),对 MN 进行认证

$$\{LBU,TS_1,\sigma_1\}_{C\text{-}HIBS\_Verify\_AR_1}.$$

如果成功,则发送认证成功消息(VA)给 MAP 通知认证结果;

2) AR_1 对 LBA 签名,发送给 MN;

④b MAP_1→*HA*:[*RBU*,$(RBU)_{MAC}$,TS_1]:

HA 检查 TS_1 的新鲜性并对 RBU 进行 HMAC 验证:$\{RBU,(RBU)_{MAC},TS_1\}_{HMAC\_Verify\_HA}$,如果成功,则更新绑定缓存,向 MN 回送 RBA;

⑤a AR_1~MAP_1:[*VA*]:

MAP_1 收到 VA 后正式更新绑定缓存,同时发送证书列表更新消息(CLU)至域内所有 AR,通知对 MN 的成功认证,CLU 消息携带 *Cert_MN*;

⑤b *HA*→MAP_1:[*RBA*,$(RBA)_{MAC}$=*HMAC*$(K_{MN\text{-}HA},RBA,TS_2)$,$TS_2$]:

MAP_1 转发 RBA 给 AR_1;

⑤c AR_1→*MN*:$[LBA,TS_3,\sigma_2=\{LBA,TS_3\}_{C\text{-}HIBS\_Sign\_AR_1}]$:

MN 首先检查 TS_3 的新鲜性,然后利用在步骤②中获得的 ID_{AR_1} 和 *Q* 值集合对 AR_1 进行认证

$$\{LBA,TS_3,\sigma_2\}_{C\text{-}HIBS\_Verify\_MN}.$$

如果成功,完成双向接入认证;

⑥a MAP_1~AR_1:[*RBA*,$(RBA)_{MAC}$,TS_2,*CLU*]:

AR_1 转发 *RBA* 给 MN 并更新 CL,增加 *Cert_MN* 表项;

⑥b MAP_1~AR_2:[*CLU*]:

AR_2 更新 CL,增加 *Cert_MN* 表项;

⑦ AR_1→*MN*:[*RBA*,$(RBA)_{MAC}$,TS_2]:

MN 检查 TS_2 的新鲜性并对 RBA 进行 HMAC 认证:$\{RBA,(RBA)_{MAC},TS_2\}_{HMAC\_Verify\_MN}$,如果成功,则完成移动注册.

(3) MN 在 MAP 域内移动

如图 2 中灰色部分所示,MN 切换至 MAP_1 域中的 AR_2,并接收到 AR_2 的 RA,其中携带 AR_2 的证书.

① AR_2→*MN*:[*RA*,*Cert_*AR_2]:

1) 由于产生域内移动,MN 仅需进行域内移动注册.MN 对 LBU 消息签名;

2) MN 随后验证 *Cert_*AR_2:$\{Cert\_AR_2\}_{Hess\text{-}IBS\_Verify\_MN}$,如果成功,则 MN 从 *Cert_*$AR_2$ 中提取 ID_{AR_2} 和 *Q* 值集合 (Q_{MAP_1},Q_{AR_2});

② *MN*→AR_2:[*LBU*,TS_4,σ_3=$\{LBU,TS_4\}_{C\text{-}HIBS\_Sign\_MN}$,*Cert_MN*]:

1) 为保证协议并行性,AR_2 首先转发 LBU 给 MAP_1;

2) AR_2 检查 TS_4 的新鲜性;

3) AR_2 检查 CL,发现存在 *Cert_MN* 表项.AR_2 无须请求 MAP_1 对 *Cert_MN* 认证,直接从 *Cert_MN* 中提取 ID_{MN} 和 *Q* 值集合,并对 MN 进行认证:$\{LBU,TS_4,\sigma_3\}_{C\text{-}HIBS\_Verify\_AR_2}$,如果成功,则发送 *VA* 给 MAP_1;

③ AR_2~MAP_1:[*LBU*]:

MAP_1 根据 LBU 临时更新绑定缓存,同时向 AR_2 回送 LBA 消息;

④ MAP_1~AR_2:[*LBA*]:

AR_2 对 LBA 签名并发送给 MN;

⑤a AR_2~MAP_1:[*VA*]:

MAP_1 正式更新绑定缓存;

⑤b $AR_2 \rightarrow MN$: $[LBA, TS_5, \sigma_4 = \{LBA, TS_5\}_{C\text{-}HIBS\_Sign\_AR_2}]$:

MN 首先检查 TS_5 的新鲜性,然后利用在步骤②中获得的 ID_{AR_2} 和 Q 值集合对 AR_2 进行认证

$$\{LBA, TS_5, \sigma_4\}_{C\text{-}HIBS\_Verify\_MN}.$$

如果成功,则完成双向接入认证和域内移动注册;

(4) MN 跨域移动

MN 产生跨 MAP 域的移动时(MN 移动至 MAP_2 域),需要重新进行家乡注册.双向接入认证协议的操作与 MN 进入 MAP_1 域时相同.

(5) M*N* 返回家乡域

MN 返回家乡域后将恢复与 HA 的信任关系,无须进行接入认证操作.

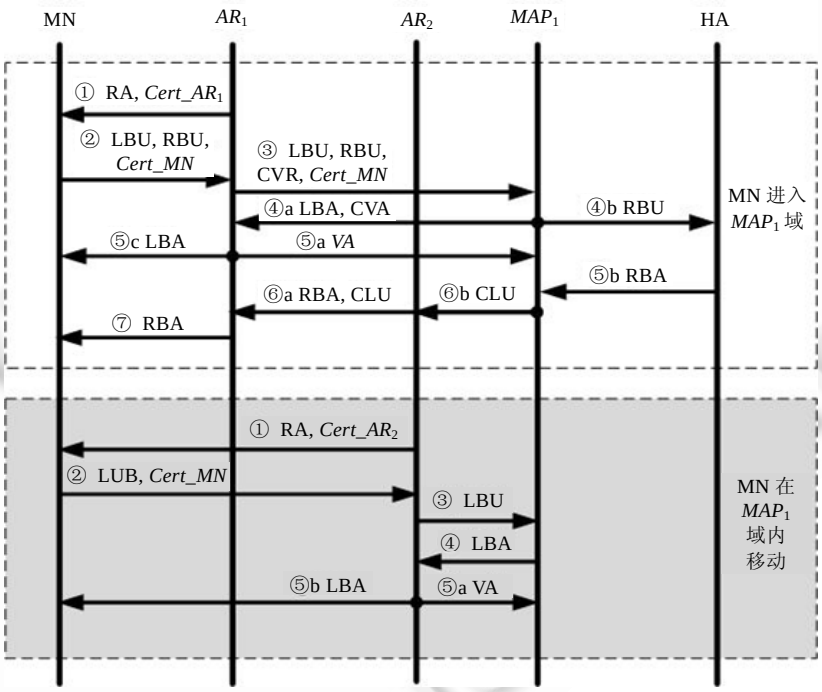

Fig.2 Flow chart of mutual access authentication

图 2 双向接入认证流程

2.4 多层HMIPv6认证扩展

双向接入认证协议应考虑 HMIPv6 下多层 MAP 嵌套的情况.C-HIBS 本身支持多层认证,需对二层认证框架和认证协议进行简单扩展,以支持多层网络环境下的双向接入认证.

将嵌套 MAP 组织成层次化的树状结构[29].其中,高层 MAP 可以管理多个低层 MAP,而每个低层 MAP 仅由一个高层 MAP 管理,AR 则位于树状结构的叶子处.图 3 为一个 t 层树状 MAP,包括 m 个 t 层 AR 和 n 个 t–1 层

MAP.结合树状结构设计多层认证框架,一层 PKG 对应于顶层 $MAP(MAP_{1,1})$,2~t–1 层 PKG 对应于相应的低层 MAP,底层用户为 t 层 AR 和 MN.完成 C-HIBS 的 Root-setup 和 Extract-cert-gen 操作后,t 层 AR 将获得由 t–1 层 MAP 颁发的证书.

当 MN 进入树状 MAP 并接入 $AR_{t,1}$,为减少跨域切换次数,选择向 $MAP_{1,1}$ 注册.MN 对 $AR_{t,1}$ 的认证过程与第 2.3 节描述过程相同,首先认证 $Cert\_AR_{t,1}$,然后基于 C-HIBS 对 $AR_{t,1}$ 进行认证.$AR_{t,1}$ 认证 MN 时需要逐层发送 CVR 至 $MAP_{1,1}$,由 $MAP_{1,1}$ 认证 $Cert\_MN$,如果认证成功,向 $AR_{t,1}$ 返回 CVA 消息.随后,$AR_{t,1}$ 对 MN 实施 C-HIBS 认证,如果成功,逐层发送 VA 给 $MAP_{1,1}$.$MAP_{1,1}$ 收到 VA 后,沿树状结构向域内所有 MAP 和 AR 发送 CLU 更新其 CL.同样基于第 2.3 节描述,当 MN 在 $MAP_{1,1}$ 域内移动时,接入 AR 可以直接对 MN 进行认证.扩展后的双向接入认证协议仍然与移动管理过程紧密结合,以确保高效性.

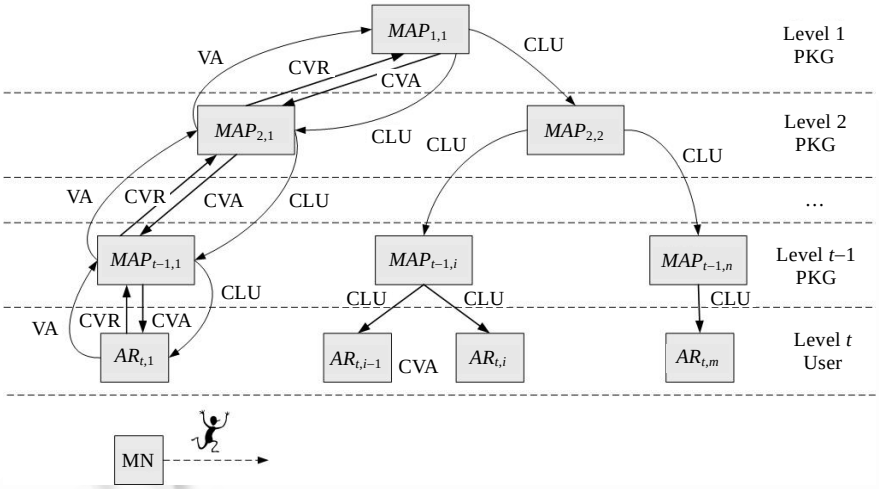

Fig.3 Multi-Level authentication framework

图 3 多层认证框架

3 讨 论

3.1 安全性分析

主要考虑以下几个方面的安全性问题:私钥保密性、签名不可伪造性、证书安全性以及移动注册安全性.

(1) 私钥保密性

在多层认证框架下,实体 E_t 的私钥(S_t=S_{t-1}+$s_{t-1}P_t$)由其父亲 PKG_{t-1} 分配,其中,s_{t-1} 为 PKG_{t-1} 私有参数.首先,对于 E_t 的祖先(父亲除外)PKG_{t-2},能够获知 S_{t-1} 和 Q_{t-1}=$s_{t-1}P_{t-2}$,而且可以根据 ID_{t-1} 计算出 P_{t-2},但要想获知 S_t,PKG_{t-2} 必须先获知 s_{t-1}.由于 s_{t-1} 为 PKG_{t-1} 的私有参数,PKG_{t-2} 只能通过 Q_{t-1} 计算 s_{t-1}.而已知 Q_{t-1} 和 P_{t-2} 计算 s_{t-1} 是计算群 G 上的 CDH(computational diffie-Hellman)[24]问题,是困难的,因此 PKG_{t-2} 无法获知 S_t;其次,对于 E_t 的兄弟 E_t' (与 E_t 处于同一管理域的实体),能够获知 $S_t'=S_{t-1}+s_{t-1}P_t'$ 和 Q_{t-1}=$s_{t-1}P_{t-2}$,而且可以根据 $ID_{E_t'}$ 和 ID_{E_t} 计算出 P_{t-2} 和 P_t.如果 E_t' 获知 s_{t-1},然后通过 S_t' 计算 S_{t-1} 就能最终计算出 S_t=S_{t-1}+$s_{t-1}P_t$.然而 E_t' 对 s_{t-1} 的计算同样涉及求解 CDH 问题,因此 E_t' 无法获知 S_t.除 PKG_{t-2} 和 E_t' 外的其他实体,由于无法获知 S_{t-1} 和 S_t',因此也无法获知 S_t.

(2) 签名不可伪造性

敌手可以通过两种方式伪造 C-HIBS 签名:攻破 C-HIBS 方案或利用之前的签名进行重放攻击.首先,C-HIBS 在签名过程中采用了 HIBS 机制.文献[27]通过严格的安全性规约推导,证明了 HIBS 在 CDH 问题困难假设下是安全的.因此,敌手无法通过攻破 C-HIBS 来伪造签名;其次,双向接入认证协议在消息签名过程中加入了时间戳,验证方可以通过时间戳方便地判别签名的新鲜性,从而有效抵御重放攻击.IETF 的现行标准[30]提

供了携带时间戳的选项(移动消息抗重放选项),可以将该选项置于 HMIPv6 移动注册消息中,增强方案的适用性.另外,基于网络时间协议[31]可以实现签名方和验证方的时间同步,以支撑时间戳机制的有效验证;同时,应尽可能缩小容忍时间窗,以提高方案工作效率.

(3) 证书安全性

证书是双向接入认证过程的主要依据,任何实体必须持有证书才能参与认证,证书的安全性至关重要.敌手可以通过伪造证书、篡改证书内容或冒用他人证书等方式对证书进行攻击.首先,实体的证书由上层 PKG 颁发并包含上层 PKG 对证书内容的 Hess-IBS 签名.由私钥保密性分析可知,敌手无法获知上层 PKG 的签名私钥,而且文献[26]证明 Hess-IBS 在 CDH 问题困难假设下是安全的,因此敌手无法伪造上层 PKG 的签名,进而无法伪造合法实体证书.同时,敌手对合法证书内容(ID,Q 值等)的篡改也可以通过对 Hess-IBS 签名的验证来识别;其次,敌手可以盗用合法实体证书以求通过 C-HIBS 验证.分析 C-HIBS 验证算法可知,尽管敌手盗用的合法证书能够通过 Hess-IBS 验证,但由于敌手无法对证书内容进行篡改,因此敌手对移动管理消息的签名将无法通过后续的 HIBS 验证,证书盗用是无效的.另外,证书中的节点类型(Type)为认证过程带来了更高的安全性.如,MAP 可以通过对 Type 的检查来判别 MN 是否具有 HA 所认定的移动能力,进一步降低敌手攻击的可能以及对 MAP 域资源的非法使用,这是签名技术所无法实现的;同时,可以通过对 Type 语义进行扩充,增强认证的灵活性.如,可以将 MN 细分为本地移动节点和跨域移动节点,当 MN 进入 MAP 域时,MAP 仅允许跨域移动节点接入.

(4) 移动注册安全性

HMIPv6 的移动注册包括域内注册(LBU/LBA)和家乡注册(RBU/RBA).MN 和 AR 分别对 LBU 和 LBA 消息进行 C-HIBS 签名和验证,确保域内注册过程的安全性.对于家乡注册,MN 在发送 RBU 时利用 MN 与 HA 共享的密钥($K_{MN\text{-}HA}$)生成$(RBU)_{MAC}$,当 HA 接收到 RBU 后,可以使用 $K_{MN\text{-}HA}$ 对$(RBU)_{MAC}$ 进行 HMAC 验证,防止针对 RBU 的欺骗攻击.另外,$(RBU)_{MAC}$ 中包含时间戳信息,避免敌手使用他人的$(RBU)_{MAC}$ 进行重放攻击.HA 对 RBA 消息作了同样的保护,保证整个家乡注册过程的安全性.

3.2 性能分析

认证延时对双向接入认证协议的高效运行至关重要.认证延时是指从 MN 进入外地网络并接收到第 1 个 RA 开始,到 MN 与接入网络的双向认证过程结束为止的时间间隔.我们首先给出分析模型,然后对 D-HMIPv6[13],2-IBS-HMIPv6[18],C-HIBS-HMIPv6(本文方案)等机制在域间切换和域内切换过程中的认证延时进行分析,最后给出分析结果.

3.2.1 分析模型

D-HMIPv6 将 Diameter 认证消息与 HMIPv6 移动注册消息紧密结合,在家乡网络和接入网络中分别设置家乡认证服务器(AAAh)和访问认证服务器(AAAf),基于挑战/应答方式实现移动注册和节点认证的并行操作,在一定程度上提高了认证性能.D-HMIPv6 仅实现了接入网络对 *MN* 的单向认证,若要实现双向接入认证,需要在 MN 和 AAAh 间增加一次消息往返(D1-HMIPv6).为进一步提升效率,也可以将双向挑战/应答全部集成在移动管理消息中,通过 MN 与 HA 间的一次消息往返完成双向接入认证(D2-HMIPv6).2-IBS-HMIPv6 基于身份签名实现了 MN 与接入网络的双向认证,将层次化移动切换过程和认证过程整合,减少了接入网络和家乡网络间的消息交互;特别是在 MN 远离家乡网络的情况下,能够体现出更高的性能.

由此可见,C-HIBS-HMIPv6 及上述方案的共同之处在于将认证消息与移动管理消息整合,以获得更高的认证效率.认证延时(T_a)主要包括认证消息的传输延时(T_t)、认证计算延时(T_c)和节点处理延时(T_p):

$$T_a=T_t+T_c+T_p \tag{1}$$

我们采用如图 4 所示的模型对 T_a 进行分析.模型中的 T_t 可以分为 3 种类型:无线链路传输延时(L_w)、域内节点传输延时(L_d)和域间节点传输延时(L_c).通常有 $L_c>L_w>L_d$,而且 L_c 与传输实体间的位置距离有密切关系

$$L_c=h\times L_d+(h-1)\times T_p \tag{2}$$

其中,h 为传输实体间的跳数,T_p 为中间路由器处理延时.

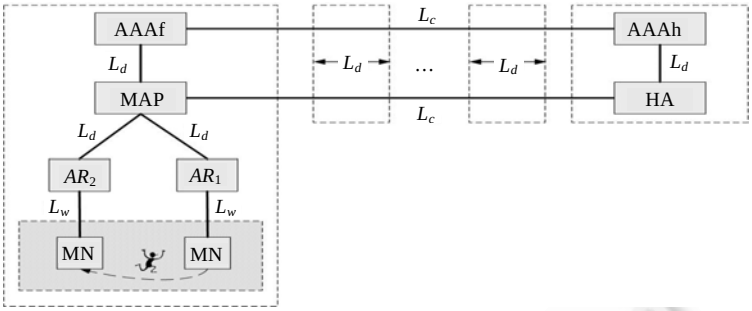

Fig.4 Analytical model of authentication latency

图 4 认证延时分析模型

T_c 除了取决于节点计算能力外,还主要决定于具体的认证方法.D-HMIPv6 中的 Diameter 协议并不给定具体的认证方法,我们假设其采用普遍的 RSA 签名算法.C-HIBS-HMIPv6 和 2-IBS-HMIPv6 均基于身份签名实现认证,相对于 RSA 签名,身份签名需要更高的计算代价.身份签名算法中主要包括的计算有:加法群上的标量乘(SM)和点加(PA)运算、乘法群上的点乘(MG)和指数(EXP)运算、双线性对(BP)运算以及 Hash 运算.我们对 C-HIBS-HMIPv6 和 2-IBS-HMIPv6 中所涉及的身份签名算法的计算量进行了分析,结果见表 2.其中,2-$IBS_{1\text{-}s/v}$ 标识 2-IBS-HMIPv6 中的一层 PKG 签名和验证算法,2-$IBS_{2\text{-}s/v}$ 标识 2-IBS-HMIPv6 中的二层用户签名和验证算法,*Hess-*$IBS_{s/v}$ 标识 Hess-IBS 签名和验证算法,*C-*$HIBS_{s/v}$ 标识 C-HIBS 签名和验证算法.所有运算均尽可能采取预计算方式,以提高运算性能.例如在 *Hess-*IBS_s 中,签名方可以提前计算 $\hat{e}(P_1,P)$,减少一次 BP 运算.另外,对于 *C-*$HIBS_v$,充分考虑了并行操作的可能,验证方的 *Hess-*IBS_v 可以在协议的并行操作过程中提前进行.

Table 2 Computational complexity analysis of identity-based signature

表 2 身份签名算法计算量分析

	SM	PA	BP	MG	EXP	Hash
2-$IBS_{1\text{-}s}$	1	1				1
2-$IBS_{1\text{-}v}$			2	1		1
2-$IBS_{2\text{-}s}$	1	1				1
2-$IBS_{2\text{-}v}$			3	2		1
Hess-IBS_s	2	1			1	1
Hess-IBS_v			1	1	1	1
C-$HIBS_s$	1	1				1
C-$HIBS_v$			2	1		1

由文献[32]可知,表 2 中计算代价较高的运算包括 BP,SM 和 EXP,而其他运算的计算代价可以忽略不计.

3.2.2 域间认证延时

当 MN 在不同 MAP 域间切换时,为完成 MN 与接入网络的双向认证,D1-HMIPv6 需要在 MN 与家乡网络间进行两次消息往返,D2-HMIPv6 则只需 1 次消息往返.

$$T_a(D1\text{-}HMIPv6)=4L_w+(4h+10)L_d+(4h+14)T_p+2t_{RSA} \tag{3}$$

$$T_a(D2\text{-}HMIPv6)=3L_w+(2h+6)L_d+(2h+9)T_p+2t_{RSA} \tag{4}$$

2-IBS-HMIPv6 需要在 MAP 和 HA 间传递 Q 值以完成双向认证过程,但 MAP 的签名过程可以与 Q 值传递过程并行,减少了 1 次一层 PKG 签名操作.

$$T_a(2\text{-}IBS\text{-}HMIPv6)=3L_w+(2h+2)L_d+(2h+5)T_p+8t_{BP}+2t_{SM} \tag{5}$$

C-HIBS-HMIPv6 基于证书和身份签名实现双向认证,认证过程中,接入网络与家乡网络不需要交互任何信息,而且 MN 对 AR 证书的验证可以同移动管理过程并行进行,即 MN 收到 AR 证书后先发送移动注册消息,再对证书进行验证,因此减少了 1 次 Hess-IBS 验证操作.

$$T_a(C\text{-}HIBS\text{-}HMIPv6)=3L_w+2L_d+5T_p+5t_{BP}+2t_{SM}+t_{EXP} \tag{6}$$

3.2.3 域内认证延时

当 MN 在 MAP 域内切换时,不需要进行家乡注册,但 D-HMIPv6 仍需要接入网络与家乡网络交互认证消息以完成双向认证,D1-HMIPv6 需要两次消息往返,D2-HMIPv6 则只需 1 次消息往返.

$$T_a'(D2\text{-}HMIPv6)=3L_w+(2h+4)L_d+(2h+7)T_p+2t_{RSA} \tag{7}$$

$$T_a'(D1\text{-}HMIPv6)=4L_w+(4h+8)L_d+(4h+12)T_p+2t_{RSA} \tag{8}$$

对于 2-IBS-HMIPv6,由于 MN 已经在 MAP 域中进行过双向接入认证,MAP 记录了 HA 的 Q 值,因此不需要在 MAP 和 HA 间传递消息.MAP 与 MN 间也不需要重新相互认证,减少了一对一层 PKG 签名和验证操作.

$$T_a'(2\text{-}IBS\text{-}HMIPv6)=3L_w+2L_d+5T_p+6t_{BP}+2t_{SM} \tag{9}$$

在 C-HIBS-HMIPv6 中,MAP 已通过 CLU 消息将 MN 的证书通知所有 AR,当新接入 AR 接收到由 MN 签名的消息后,先转发 LBU 至 MAP,再对 MN 签名进行验证,保证协议的并行性.

$$T_a'(C\text{-}HIBS\text{-}HMIPv6)=3L_w+3T_p+4t_{BP}+2t_{SM} \tag{10}$$

3.2.4 分析结果

用 t_x 标识 x 运算的计算时间,综合文献[33–36]的分析和实验数据,在相同的计算资源和等价的安全性前提下,可以得出如下结论:

$$t_{BP}=1.5\sim3t_{RSA},t_{SM}=t_{EXP}=0.25\sim1t_{RSA} \tag{11}$$

另外,参考文献[18]设定模型中的参数值:L_w=4ms,L_d=2ms,T_p=0.5ms.在满足公式(11)的条件下,取 4 组 t_{BP} 和 t_{SM} 值($\langle t_{BP}=3t_{RSA},t_{SM}=1t_{RSA}\rangle$,$\langle t_{BP}=2.5t_{RSA},t_{SM}=0.75t_{RSA}\rangle$,$\langle t_{BP}=2t_{RSA},t_{SM}=0.5t_{RSA}\rangle$,$\langle t_{BP}=1.5t_{RSA},t_{SM}=0.25t_{RSA}\rangle$)对域间认证延时进行分析,结果如图 5 所示.

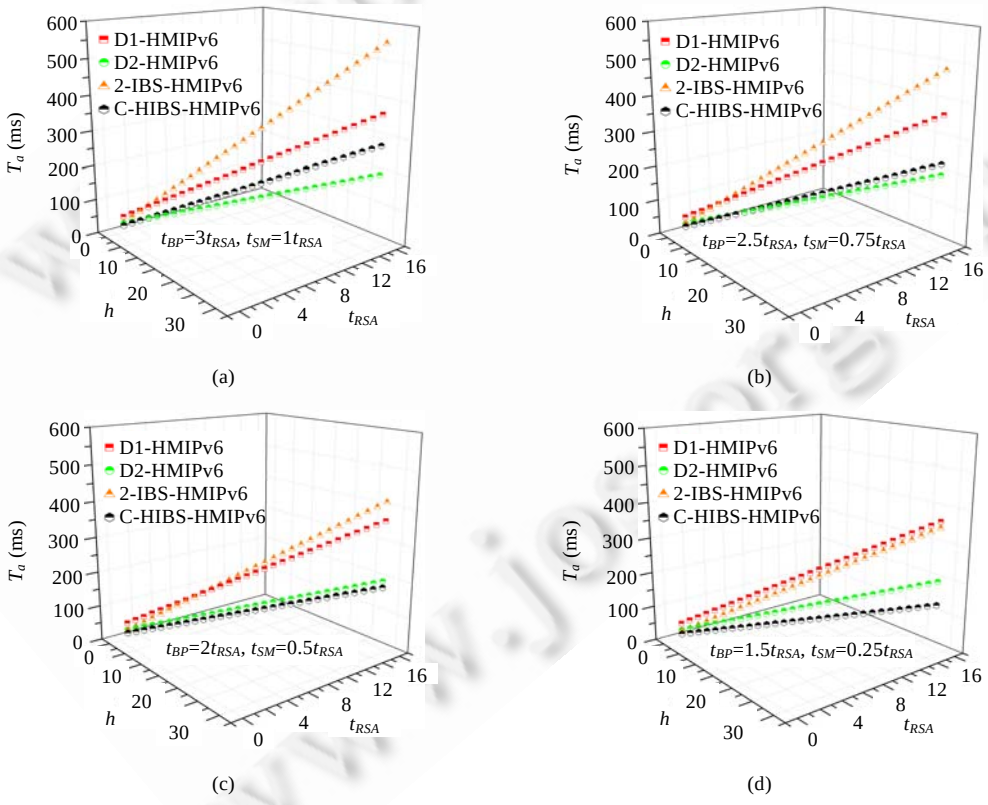

Fig.5 Inter-Domain authentication latency

图 5 域间认证延时

在域间认证过程中,D1-HMIPv6,D2-HMIPv6 和 2-IBS-HMIPv6 均需要在接入网络和家乡网络间交互消息.其中:

- 2-IBS-HMIPv6 需要 1 次消息往返且包含大量 BP 和 SM 运算,导致 h 和 t_{RSA} 值偏高,因此在绝大多数情况下 T_a 较高;
- 尽管 D1-HMIPv6 需要 2 次消息往返,但仅需两次 RSA 签名和验证(t_{RSA} 值低),T_a 在大部区间内优于 2-IBS-HMIPv6;然而随着 BP 和 SM 运算性能的提升,如图 5(d)所示,在 t_{BP}=1.5t_{RSA},t_{SM}=0.25t_{RSA} 的情况下,2-IBS-HMIPv6 的 T_a 已开始优于 D1-HMIPv6;
- D2-HMIPv6 仅需要一次消息往返且 t_{RSA} 值低,T_a 要明显优于 D1-HMIPv6 和 2-IBS-HMIPv6.

C-HIBS-HMIPv6 消除了消息往返,但仍需要一定的 BP 和 SM 运算,当运算性能较低时,其 T_a 高于 D2-HMIPv6(如图 5(a)、图 5(b)所示);然而随着 BP 和 SM 运算性能的提升,如图 5(c)所示,在 t_{BP}=2t_{RSA},t_{SM}=0.5t_{RSA} 的情况下,C-HIBS-HMIPv6 的 T_a 完全优于其他 3 种机制.

采用与域间认证延时分析相同的 4 组 t_{BP} 和 t_{SM} 取值,得到域内认证延时分析结果,如图 6 所示.对于域内认证,2-IBS-HMIPv6 和 C-HIBS-HMIPv6 消除了消息往返,而 D1-HMIPv6 和 D2-HMIPv6 同域间认证相比基本没有变化.尽管 2-IBS-HMIPv6 仍然包含一定的 BP 和 SM 运算,但即便在运算性能较低的情况下(如图 6(a)所示),其 T_a 已优于 D1-HMIPv6.如图 6(d)所示,当 t_{BP}=1.5t_{RSA},t_{SM}=0.25t_{RSA} 且 t_{RSA}<5.5ms 时,2-IBS-HMIPv6 的 T_a 甚至开始优于 D2-HMIPv6.在域内认证过程中,C-HIBS-HMIPv6 进一步减少了 BP 和 SM 运算次数,而且协议的并行性使得域内传输延时得到降低,因此如图 6(b)所示,当 t_{BP}=2.5t_{RSA},t_{SM}=0.75t_{RSA} 时,C-HIBS-HMIPv6 的 T_a 开始优于其他 3 种机制;且随着 h 的增加和 t_{RSA} 的下降,优势逐渐明显.

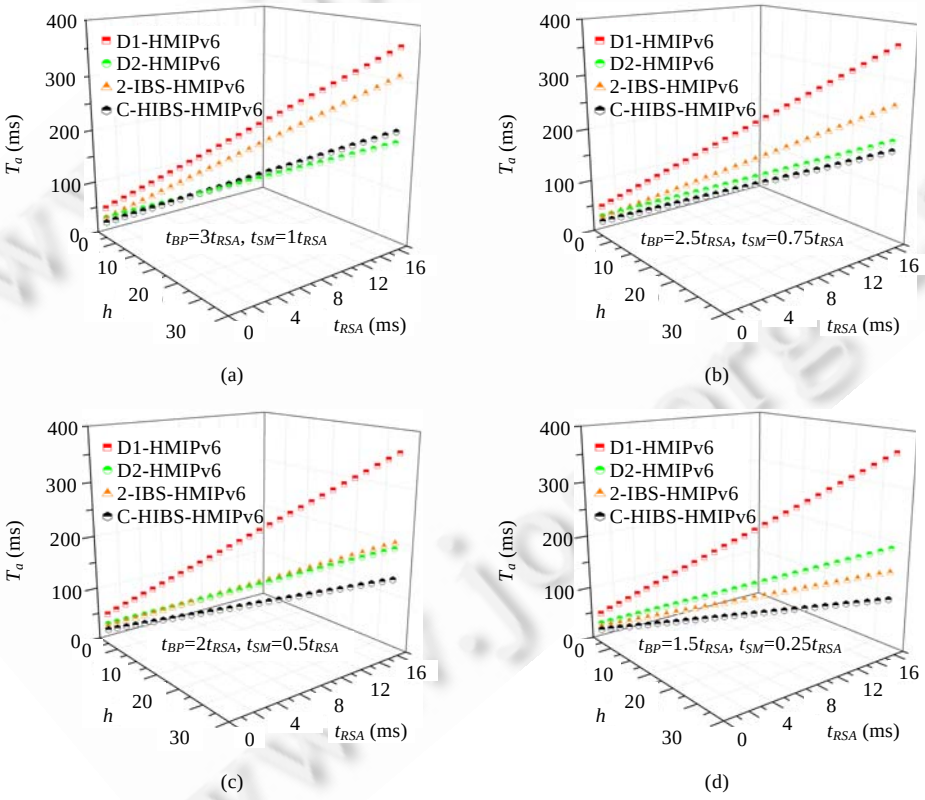

Fig.6 Intra-Domain authentication latency

图 6 域内认证延时

综上所述,4 种机制的认证延时主要取决于 h 和计算性能,后者包括 RSA,BP 和 SM 等运算.在 h 和计算性能较低的情况下,C-HIBS-HMIPv6 无法完全发挥出其优势;但随着身份签名算法的不断优化及硬件工艺的快速发展,节点的计算性能必然会不断提升,例如文献[37]中基于 FPGA 的 BP 计算仅需 1.07ms.

另外,当家乡网络和接入网络距离较远时(h>20),消除了消息往返,C-HIBS-HMIPv6 的认证延时要明显优于其他 3 种机制.因此,当 MN 的移动远离家乡网络时,无论域间认证还是域内认证,C-HIBS-HMIPv6 的性能都是最优的.

4 结束语

本文提出了一种基于证书和身份的 HMIPv6 网络认证机制,在分层框架下,采用节点证书与基于身份签名相结合的方式实现了用户与接入网络的双向认证.

- 该机制以分级网络访问标识符作为用户公钥,降低了 PKI 体系下密钥管理和维护的复杂度;
- 以定义的节点证书为认证主要依据,消除了传统 AAA 框架中接入网络与家乡网络间的消息交互;
- 基于节点证书设计了层次化身份签名方案,通过将认证过程与移动管理过程有机整合,提高了机制的工作效率;
- 该机制能够经过简单扩展支持多层 HMIPv6 网络下的接入认证.

性能分析表明,当节点在远离家乡的外地网络移动时,本文的方案明显优于其他方案.

如何通过基于身份的签密方法[38]在认证过程中实现对用户数据的机密性保护,同时降低系统整体开销,将成为下一步研究工作的主要内容.

致谢 在此向对本文的工作给予支持和建议的老师和同学表示衷心感谢.

References:

[1] Perkins C, Johnson D, Arkko J. Mobility support in IPv6. RFC6275, 2011.

[2] Soliman H, Castelluccia C, Elmalki K, Bellier L. Hierarchical mobile IPv6 (HMIPv6) mobility management. RFC5380, 2008.

[3] Adams C, Farrell S, Kause T, Mononen T. Internet X.509 public key infrastructure certificate management protocol (CMP). RFC4210, 2005.

[4] Laat C, Gross G, Gommans L, Vollbrecht J. Generic AAA architecture. RFC2903, 2000.

[5] Arkko J, Devarapalli V, Dupont F. Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents. RFC3776, 2004.

[6] Kaufman C. Internet key exchange (IKEv2) protocol. RFC4306, 2005.

[7] Mizuno S, Koga J, Ohwada H, Suzuki K. PKI support in hierarchical mobile IPv6. Draft-mizuno-mobileip-hmipv6-pki-00.txt, 2003.

[8] Feng B, Robert D, Ying Q. Certificate-Based binding update protocol (CBU). Draft-qiu-mip6-certificated-binding-update-03.txt, 2005.

[9] Giaretta G, Guardini I, Demaria E, Bournelle J, Lopez R. Authentication, authorization, and accounting (AAA) goals for mobile IPv6. RFC5637, 2009.

[10] Korhonen J, Bournelle J, Tschofenig H, Perkins C, Chowdhury K. Diameter mobile IPv6: Support for network access server to diameter server interaction. RFC5447, 2009.

[11] Korhonen J, Tschofenig H, Bournelle J, Giaretta G, Nakhjiri M. Diameter mobile IPv6: Support for home agent to diameter server interaction. RFC5778, 2010.

[12] Fajardo V, Arkko J, Loughney J, Zorn G. Diameter base protocol. Draft-ietf-dime-rfc3588bis-29.txt, 2011.

[13] Paal E, Thomas H, Frederic P. Authenticated access for IPv6 supported mobility. In: Proc. of the IEEE Int'l Symp. on Computers and Communication (ISCC 2003). 2003. 569−575. [doi: 10.1109/ISCC.2003.1214179]

[14] Xiao WS, Zhang YJ, Li ZC. Hierarchical AAA in mobile IPv6 networks. Journal on Communications, 2006,27(2):51−55 (in Chinese with English abstract).

[15] Haddad W, Krishnan S, Soliman H. Using cryptographically generated addresses (CGA) to secure HMIPv6 protocol (HMIPv6sec). Draft-haddad-mipshop-hmipv6-security-06, 2006.

[16] Ramanarayana K, Jacob L. A secure IPv6-based urban wireless mesh network (SUMNv6). Computer Communications, 2008,31(15): 3707−3718. http://dx.doi.org/10.1016/j.comcom.2008.07.003

[17] Tian Y, Zhang YJ, Liu Y, Li ZC. A fast authentication mechanism using identity based signature in mobile IPv6 network. Journal of Software, 2006,17(9):1800−1888 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1800.htm [doi: 10.1360/jos171980]

[18] Tian Y, Zhang YJ, Zhang HW, Li ZC. Identity-Based hierarchical access authentication in mobile IPv6 network. Chinese Journal of Computers, 2007,30(6):905−915 (in Chinese with English abstract).

[19] Lee BG, Kim HG, Sohn SW, Park KH. Concatenated wireless roaming security association and authentication protocol using ID-based cryptography. In: Proc. of the 57th IEEE Semiannual Vehicular Technology Conf. (VTC 2003), Vol.3. Spring-Verlag, 2003. 1507−1511. http://dx.doi.org/10.1109/VETECS.2003.1207072

[20] Arkko J, Kempf J, Zill B, Nikander P. Secure neighbor discovery (SEND). RFC3971, 2005.

[21] Aura T. Cryptographically generated addresses (CGA). RFC3972, 2005. [doi: 10.1007/10958513_3]

[22] Jung HY, Soliman H, Koh SJ, Lee JY. Fast handover for hierarchical MIPv6 (F-HMIPv6). Draft-jung-mobopts-fhmipv6-00.txt, 2005.

[23] Shamir A. Identity-Based cryptosystems and signature schemes. In: Advances in Cryptology—Crypto'84. LNCS 196, Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[24] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. SIAM Journal of Computing, 2003,32(3):586−615. http://dx.doi.org/10.1137/S0097539701398521

[25] Antoine J. The Weil and Tate pairings as building blocks for public key cryptosystems survey. In: Proc. of the 5th Int'l Symp. on Algorithmic Number Theory (ANTS-V). LNCS 2369, 2002. 11−18. [doi: 10.1007/3-540-45455-1_3]

[26] Hess F. Efficient identity based signature schemes based on pairings. In: Proc. of the SAC 2002. LNCS 2595, 2003. 310−324. [doi: 10.1007/3-540-36492-7_20]

[27] Craig G, Alice S. Hierarchical ID-based cryptography. In: Proc. of the 8th Int'l Conf. on the Theory and Application of Cryptology and Information Security. LNCS 2501, 2002. 149−155. [doi: 10.1007/3-540-36178-2_34]

[28] Krawczyk H, Bellare M, Canetti R. HMAC: Keyed-Hashing for message authentication. RFC2104, 1997.

[29] Gao TH, Guo N, Zhao H. Study of mobile IPv6 seamless and real-time handover policy based on tree-style MAP. Journal on Communications, 2004,25(11):98−106 (in Chinese with English abstract).

[30] Patel A, Leung K, Khalil M, Akhtar H, Chowdhury K. Authentication protocol for mobile IPv6. RFC4285, 2006.

[31] Mills D, Delaware U, Martin J, Burbank J, Kasch W. Network time protocol version 4: Protocol and algorithms specification. RFC5905, 2010.

[32] Sandip V, Subhash C. Threshold signature cryptography scheme in wireless ad-hoc computing. Contemporary Computing, 2009, 40(7):327−335. [doi: 10.1007/978-3-642-03547-0_31]

[33] Barreto PSLM, Ben L, Michael S. Efficient implementation of pairing-based cryptosystems. Journal of Cryptology, 2004,17(4): 321−334. [doi: 10.1007/s00145-004-0311-z]

[34] Barreto PSLM, Kim HY, Ben L, Michael S. Efficient algorithms for pairing-based cryptosystems. In: Proc. of the 22nd Annual Int'l Cryptology Conf. on Advances in Cryptology. LNCS 2442, 2002. 354−368. [doi: 10.1007/3-540-45708-9]

[35] Elisavet K. Efficient cluster-based group key agreement protocols for wireless ad hoc networks. Journal of Network and Computer Applications, 2011,34(1):384−393. http://dx.doi.org/10.1016/j.jnca.2010.05.001

[36] Xiong X, Wong DS, Deng X. Tiny pairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks. In: Proc. of the WCNC 2010. 2010. 1−6.

[37] Sylvain D, Nicolas G. A FPGA pairing implementation using the residue number system. Cryptology ePrint Archive, 2011. http://eprint.iacr.org/2011/176

[38] Malone-Lee J. Identity-Based signcryption. Cryptology ePrint Archive, 2002. http://eprint.iacr.org/2002/098

附中文参考文献:

[14] 肖文曙,张玉军,李忠诚.移动 IPv6 网络的层次 AAA 方案研究.通信学报,2006,27(2):51−55.

[17] 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. http://www.jos.org.cn/1000-9825/17/1800.htm [doi: 10.1360/jos171980]

[18] 田野,张玉军,张瀚文,李忠诚.移动 IPv6 网络基于身份的层次化接入认证机制.计算机学报,2007,30(6):1−11.

[29] 高天寒,郭楠,赵宏.基于树状 MAP 的移动 IPv6 无缝实时切换策略研究.通信学报,2004,25(11):98−106.

高天寒(1978－),男,辽宁沈阳人,博士,副教授,主要研究领域为下一代互联网,网络安全.

郭楠(1977－),女,博士,副教授,主要研究领域为计算机网络管理,服务计算.

朱志良(1962－),男,博士,教授,博士生导师,CCF 会员,主要研究领域为计算机网络与通信,混沌分形与数据处理.