ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.9, September 2006, pp.1980−1988
DOI: 10.1360/jos171980

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

移动 IPv6 网络基于身份签名的快速认证方法*

田 野[1,2+], 张玉军[1], 刘 莹[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 100049)

A Fast Authentication Mechanism Using Identity Based Signature in Mobile IPv6 Network

TIAN Ye[1,2+], ZHANG Yu-Jun[1], LIU Ying[1,2], LI Zhong-Cheng[1]

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

[2](Graduate School, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: Phn: +86-10-62565533 ext 9228, E-mail: jack_ty@ict.ac.cn, http://www.ict.ac.cn

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):1980−1988. http://www.jos.org.cn/1000-9825/17/1980.htm

Abstract: Access authentication is important to the deployment and application of mobile IPv6 network, and Authentication in handover procedure will reduce handover performance in mobile IPv6 network. However, many studies for the access authentication in mobile IPv6 network ignore the effect of authentication in handover procedure. Furthermore, many certificate-based authentication schemes are not fit for the wireless mobile environment. To solve these drawbacks, a fast mutual authentication mechanism using Identity-based signature in mobile IPv6 network is proposed. The identity-based signature scheme uses NAI (network access identifier) as public key and simplifies the key management in wireless mobile environment, so it can resolve the deficiency in PKI-based authentication mechanism. An effective combination of the fast handover and authentication can minimize the additional load resulting from authentication in mobile procedure. Performance analysis results show that the proposed mechanism is more efficient than other schemes.

Key words: mobile IPv6 network; fast authentication; identity based signature; fast handover

摘 要: 接入认证对移动 IPv6 网络的部署和应用至关重要,在切换过程中加入认证过程会影响移动 IPv6 网络的切换性能.当前,对移动 IP 网络中接入认证的研究大多没有考虑对切换性能的影响.另外,目前许多双向认证机制都是基于证书的方式来实现,无线移动环境的特殊性使得这种方式并不适合无线移动网络.一种适用于移动 IPv6 网络的基于身份签名的快速双向认证方法被提了出来.该方法使用 NAI(network access identifier)作为公钥,简化了无线移动环境中的密钥管理问题,有效地解决了基于 PKI(private key infrastructure)的认证机制的不足.同时,该方法有效结合了快速切换和接入认证过程,降低了移动过程中由于引入接入认证带来的额外开销.最后,通过性能分析证明该方法比其他方法更有效.

* Supported by the National Natural Science Foundation of China under Grant No.90604014 (国家自然科学基金); the Innovation Funding from the Institute of Computing Technology, the Chinese Academy of Sciences under Grant No.20056350 (中国科学院计算技术研究所创新课题)

Received 2005-05-25; Accepted 2005-12-31

关键词: 移动 IPv6 网络;快速认证;基于身份签名;快速切换
中图法分类号: TP393 文献标识码: A

在无线移动 IPv6 网络中,减少切换延时是其中最主要的问题之一.移动 IPv6 协议[1]只解决了 MN(mobile node)从一个 AR(access router)移动到另一个 AR 时如何保持连接的问题,而并没有考虑到移动切换过程中产生的大量延时远不能满足实时应用的需求.因此,一种增强型移动 IPv6 协议——快速切换协议[2]被了提出来.该协议采用预切换机制,通过二层触发的方式降低 MN 在无线移动 IPv6 网络中的切换延时.

无线网络环境的开放性特点使得安全问题尤为重要,尤其需要对接入网络的用户身份进行认证.而 AAA (authentication, authorization and accounting)协议(如 diameter)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,并没有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)和 AAA 解决安全性问题的方法[3].

切换和认证往往同时发生,在切换过程中引入认证会不可避免地增加切换延时.为了解决这个问题,文献[4]提出了一种基于 IEEE 802.1x 模型的预测认证方法以实现快速切换;文献[5]提出了一种结合快速切换协议和 AAA 协议的方法实现快速认证.这两种方法都考虑了如何结合认证和切换过程,但却忽略了认证框架下所采用的具体认证方法.Diameter 协议建议采用 EAP(extensible authentication protocol)实现认证功能[6],而 EAP 协议[7]作为一个基于请求/应答方式的认证框架,它提供了一种支持各种具体认证方法的标准机制.因此,在采用 EAP 协议实现认证的各种方法中,认证处理时间和安全级别(是否支持双向认证)由具体认证方法决定.目前,支持双向认证的认证方法大多数都是基于公钥证书实现的[8,9],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.因此,在无线移动环境中采用证书机制是不合适的.

相反地,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.基于上述特点,文献[10]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.为了简化密钥管理,该方法采用 NAI(network access identifier)作为公钥,它的格式是 username@homedomain.这种方法有效地解决了上述基于 PKI 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.

本文提出了一种基于身份签名的快速认证机制.该机制利用基于身份签名方案的特性,将快速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 Diffie-Hellman 问题基础上的,具有足够的安全性.

本文第 1 节简单介绍移动 IPv6 快速切换协议、一种基于移动 IPv6 的 AAA 认证机制和具体认证框架以及基于身份的密码学.第 2 节设计一种基于身份的签名机制并重点阐述基于身份签名的快速认证方案.第 3 节给出相应的性能分析.最后总结本文并给出下一步工作.

1 相关背景

1.1 移动**IPv6**的快速切换协议

移动 IPv6 实现了 MN 从一个 AR 移动到另一个 AR 时如何保持连接的功能.在这个切换过程中,由于链路切换和 IP 协议的某些操作(如转交地址的配置、绑定更新等),使得移动节点无法发送和接收任何数据包,从而导致移动 IPv6 协议无法满足实时应用的需求(如 VoIP 等).为了解决这个问题,尽可能地减少切换延时,IETF 提出了一种快速切换的方案,该方案的实现流程如图 1 所示.

当 MN 发现新的链路可用时(在 WLAN 中,MN 通过链路层信号扫描实现),它将发送新链路前缀请求消息(router solicitation for proxy advertisement,简称 RtSolPr)给当前链路的接入路由器(PAR),请求新链路的子网信

息.在收到PAR的回应消息(proxy router advertisement,简称PrRtAdv)后,MN将配置适用于新链路的CoA(care of address),而此时,MN仍然在当前链路上.通过这个过程,移动IPv6中的新子网前缀发现延时被消除了.

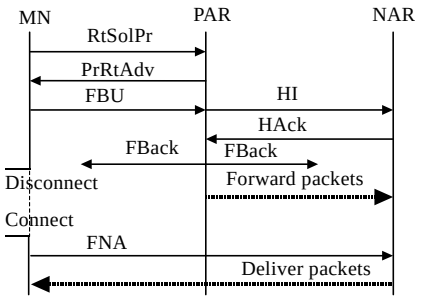


Fig.1 Fast handover flow for mobile IPv6

图1 移动IPv6快速切换实现流程

在配置好新的CoA后,MN在当前链路发送FBU(fast binding update)消息,在PAR和NAR之间建立一条隧道.隧道建立好后,PAR将发往MN的当前CoA地址的数据包通过隧道转发到MN的新CoA地址(在NAR上缓存).PAR通过HI/Hack (handover initiate/handover acknowledge)消息检查MN的新CoA的可用性.

若MN在当前链路收到PAR的FBack(fast binding acknowledgment)消息,在MN接入新链路后,直接发送FNA(fast neighbor advertisement)消息通知NAR. NAR将缓存的发往MN的新CoA地址的数据包转发给MN.若MN发送FBU消息后发生链路切换,即在当前链路没有收到PAR的FBack消息,则MN在接入新链路后,将FBU消息封装在FNA消息中发送给NAR. NAR收到该消息后,将转发FBU给PAR,重新建立隧道,并通知PAR转发发往MN的消息.

1.2 基于移动IPv6的AAA认证机制

本节中,我们介绍一种基于移动IPv6的AAA认证机制[3],如图2所示.

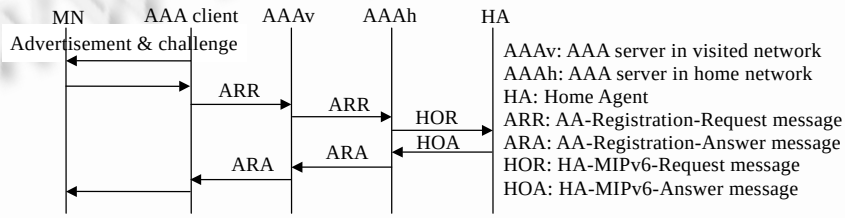


Fig.2 AAA authentication architecture in mobile IPv6

图2 移动IPv6的AAA认证框架

MN接入新的网络时,通过AAAv与AAAh进行交互(ARR/ARA),实现认证.为了提高效率,MN还可以将相应注册信息携带在ARR中,实现认证的同时完成与HA的注册.该框架虽然实现了AAA认证框架与移动IPv6的结合,但却忽略了如何具体完成认证.即使采用最简单的EAP-MD5单向认证方法,完成整个认证过程至少还需要增加一次MN与AAAh的交互.而若需要实现双向认证,则增加的交互次数会更多(如图3所示).这就极大地降低了MN异地接入的效率,尤其是在移动切换过程中表现得会更加明显.

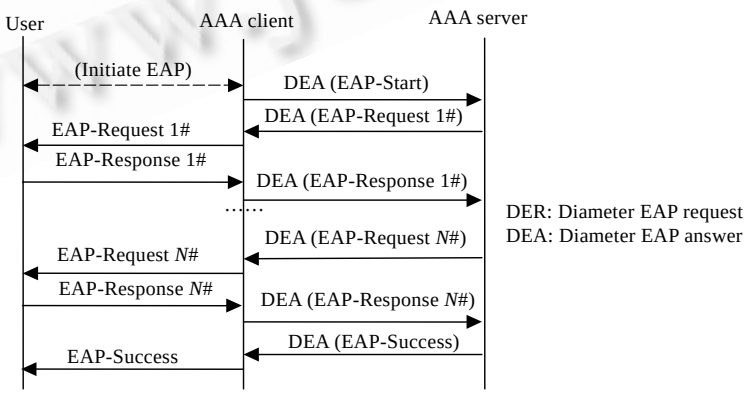


Fig.3 EAP authentication architecture for diameter

图3 Diameter EAP认证框架

1.3 基于身份的密码方案

基于身份密码学(IBC)最初是为了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[11].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——PKG (private key generator),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,但并没有能够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[12].此后,一些应用对技术的基于身份签名方案也相继被提了出来[13−15].这些方案的安全性大多是基于某种 Diffie-Hellman 问题,如 CDHP(computational diffie-hellman problem)[13,14]或 BDHP(bilinear diffie-hellman problem)[15]等.由于这些方案都是在对技术基础上实现的,下面简单介绍对技术.

本文使用与文献[12]中相同的符号.设 p,q 为素数,满足 $p=2 \bmod 3$ 和 $p=6q+1$.设 E 为 F_p 上的超奇异椭圆曲线:$y^2=x^3+1$.群上有理数点 $E(F_p)=\{(x,y)\in F_p\times F_p:(x,y)\in E\}$形成一个阶为 $p+1$ 的循环群.由于 $p+1=6q$,设 G_1 为阶为 q 的循环子群.设 P 为 G_1 的生成元,G_2 是 $F_{p^2}^*$ 中所有阶为 q 的元素组成的子群.一类修正的 Weil 对[12]为

$$\hat{e}:G_1\times G_1\to G_2 \tag{1}$$

该对满足如下性质:

- 双线性:对于所有的 $P,Q\in G_1$,所有的 $a,b\in Z$,满足 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$.同时,对任意 $P_1,P_2,Q\in G_1$,有 $\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\times\hat{e}(P_2,Q)$.
- 非退化性:若 P 为 G_1 的生成元,则 $\hat{e}(P,P)\in F_{p^2}^*$ 为 G_2 的生成元.
- 实效性:对于所有的 $P,Q\in G_1$,存在一种有效算法计算 $\hat{e}(P,Q)\in G_2$.

2 基于身份签名的快速认证协议

本节中,我们首先设计一种基于身份的签名方案(IBS),然后在此基础上提出一种基于身份签名技术的快速认证协议.

2.1 基于身份的签名方案

由于移动终端计算能力有限,因此在设计签名方案时,应尽可能地减少移动终端的计算.所以,本签名方案将更繁重的计算(如 Weil 对运算)放在了验证阶段.

(1) 系统参数的建立(由 PKG 执行):

- 随机选择一个数 $s\in Z_q^*$,计算 $P_{pub}=sP$,其中 P 为 G_1 的生成元;
- 选择两个强密码杂凑函数 $H_1:\{0,1\}^*\to Z_q^*$ 和 $H_2:\{0,1\}^*\to G_1^*$,其中,H_1 将任意长度输入映射到固定长度;H_2 把用户身份 ID 映射到 G_1 中一个元素.具体实现可参考文献[15];
- 最后,PKG 把 s 作为系统的私钥保存,并公开系统参数$\langle G_1,G_2,\hat{e},P,P_{pub},H_1,H_2,p,q\rangle$.

(2) 用户密钥生成(由 PKG 执行):

- 给定任一身份 $ID\in\{0,1\}^*$,计算公钥 $Q_{ID}=H_2(ID)$;
- 计算私钥 $d_{ID}=sQ_{ID}$,其中 s 为系统私钥.

(3) 签名:为了使用私钥 d_{ID} 对消息 $M\in\{0,1\}^*$签名,签名者需要执行:

- 随机选择 $r\in Z_q^*$,计算 $R=rP$;
- 输出针对 M 的签名:$\sigma=(R,rP_{pub}+H_1(M,R)\cdot d_{ID})$.

(4) 验证:设$\sigma=(U,V)$为针对 M 的签名,验证者需要执行:

- 计算 $Q_{ID}=H_2(ID)$;
- 计算 $u=\hat{e}(V,P)$;
- 计算 $v=\hat{e}(U+H_1(M,U)Q_{ID},P_{pub})$;

- 若 $u=v$,输出接受;否则输出拒绝.

上述结果是很容易被验证的:若$\sigma=(U,V)$是针对消息 M 的基于某个身份 ID 的有效签名,则

$$\begin{aligned} v &=\hat{e}(U+H_1(M,U)Q_{ID},P_{pub})\\ &=\hat{e}(U,P_{pub})\times\hat{e}(H_1(M,U)Q_{ID},P_{pub})\\ &=\hat{e}(rP_{pub},P)\times\hat{e}(H_1(M,U)d_{ID},P)\\ &=\hat{e}(rP_{pub}+H_1(M,U)d_{ID},P)\\ &=u. \end{aligned}$$

该方案的安全性的形式化证明可参考文献[12],这里不再具体介绍.

2.2 快速认证协议设计思想

在现有 EAP 认证框架下,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(如图 3 所示),认证延时将随着交互次数的增多而显著增大.由签名机制的特点,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.

另外,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 AAA 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,任何节点均可以很容易地获取.利用这一特点,就可以实现 MN 直接与接入网络的 AAAv 交互完成接入认证,从而消除 AAAv 与 AAAh 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.

基于上述分析和考虑,本节提出一种基于身份签名技术的快速认证协议.系统实现模型如图 4 所示.在 MN 执行快速绑定更新过程中,通知 NAR 和 NAAAv 向 MN 的 AAAh 请求 MN 的签名参数(SPR/SPA 消息).当 MN 进入新访问域时,只需和 AAAv 进行一次交互,完成接入认证过程,同时通过与 HA 交互完成绑定更新过程.

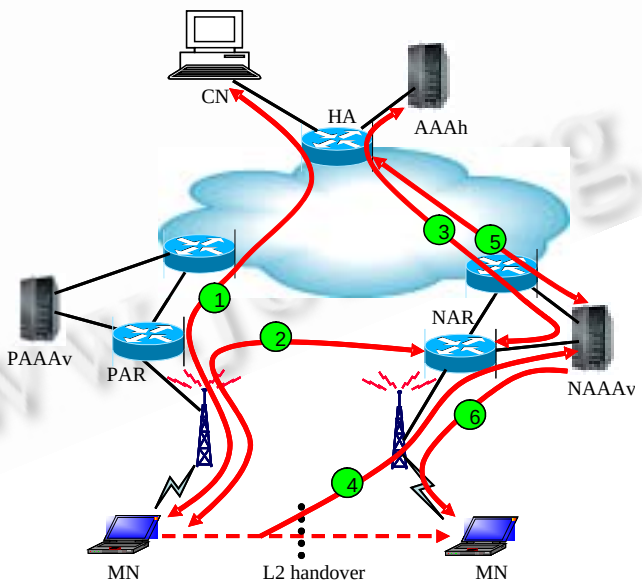


Fig.4 Proposed system model

图 4 系统模型

在描述协议的具体实现之前,我们规定如下设计准则:

- 协议要求 MN 和 AAA 服务器均支持基于身份签名技术,其身份 ID 为 NAI,且每个实体都有一个与其 NAI

对应的私钥;

- AAA 服务器完成认证功能,但它并非 PKG.而 PKG 可以采用离线方式避免某些攻击;
- 为了抵抗重放攻击,每个签名消息必须携带时间戳.

2.3 快速认证实现流程

协议具体实现如图 5 所示.消息交互过程可分为两个阶段:第 1 阶段,MN 发送携带 AS 的 FBU 消息开始快速切换,同时触发 NAR/AAAv 发送 SPR 消息获得 MN 的签名参数$\langle G_1,G_2,\hat{e},P,P_{pub},H_1,H_2,p,q\rangle$;第 2 阶段,当 MN 收到 FBack 后,开始接入认证和绑定更新.具体描述如下:

(1) MN→NAR:AReq=$\langle BU||TS_1||\{BU||TS_1\}Sign_{mn}\rangle$;

(2) NAR→AAAv:ARR=⟨AReq-AVP⟩;

(3) AAAv→HA:HOR=⟨BU-AVP⟩:

- AAAv 验证$\{BU||TS_1\}Sign_{mn}$,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 AAAv 对 MN 的认证;
- 为了提高效率,AAAv 先发送 HOR 消息,然后验证签名,从而实现绑定更新与验证的并发执行;

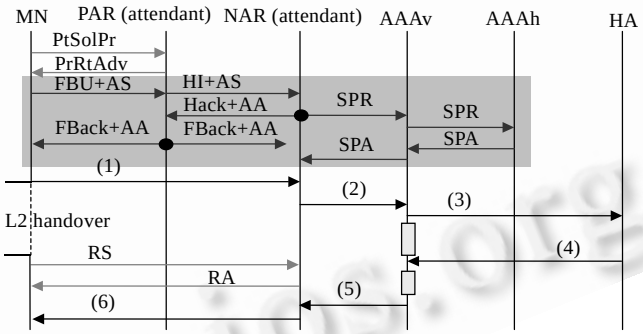
(4) HA→AAAv:HOA=⟨BA-AVP⟩;

(5) AAAv→NAR:ARA=⟨ARsp-AVP⟩;

- AAAv 签名 BA (binding acknowledge)消息,即 ARsp=$\langle BA||TS_2||\{BA||TS_2\}Sign_{aaav}\rangle$;

(6) NAR→MN:Arsp:

- MN 验证$\{BA||TS_2\}Sign_{aaav}$,同时检查时间戳 TS_2,保证签名消息的新鲜性;
- 当验证成功后,完成 MN 对接入网络的认证,从而实现双向认证;
- 为提高切换效率,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.



AS: Attendant solicit message piggyback the NAI of MN
AA: Attendant advertisement message
SPR: MN signature-parameters-request message
SPA: MN signature-parameters-answer message
RS: Router solicitation message
RA: Router advertisement message

Fig.5 Fast authentication protocol using IBS

图 5 基于 IBS 的快速认证协议

3 性能分析

为了分析协议效率,我们设计了一种简单切换延时性能分析模型,比较本文提出的协议 IBS-FAMIPv6 和 Kim 等人提出的 FAMIPv6 协议[5]的切换延时.这里,定义切换延时是从 MN 在前一访问域发送最后一个数据包 AReq 开始,到 MN 在新访问域收到 BA 消息为止的一段时间间隔.

FAMIPv6 协议[5]通过结合快速切换协议[2]和一种基于移动 IPv6 的 AAA 认证机制[16],有效降低了认证带来的额外开销.但该协议将认证与绑定更新分离,认证完成后还需要执行 MN 与 HA 的绑定更新才能完成整个切

换过程.同时,该协议基于文献[16]提出的认证方案,使用 RSA 签名机制只实现了网络对用户的认证.

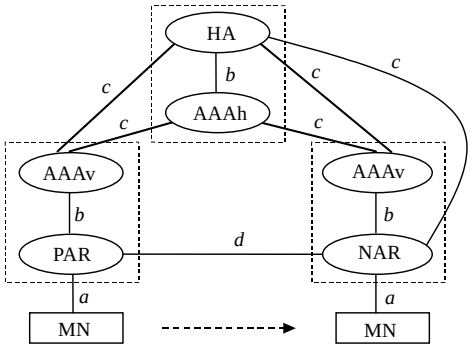


Fig.6 System model for handover latency analysis

图 6 切换延时分析模型

如图 6 所示,设两节点之间传输延时分别为 a,b,c,d.设数据包在任一节点的处理时间为 t_p,这里,t_p并不包括节点签名/验证的处理时间.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 IBS 机制签名/验证所需时间为 t_s/t_v.

IBS 机制的处理性能主要由两个操作决定:一个是椭圆曲线上的点乘操作;另一个是第 1 节定义的 Weil 对操作.根据第 2.1 节介绍,IBS-FAMIPv6 机制的签名阶段需要进行 3 次点乘和 1 次 hash 运算,而验证阶段需要 2 次 Weil 对、1 次点乘和 1 次 hash 运算.当 MN 在子网间频繁移动时,可以通过预计算 rP 和 rP_{pub} 减少签名阶段的点乘运算次数,经过优化后的签名阶段只需要进行 1 次点乘和 1 次 hash 运算.根据文献[17]的介绍,计算 512-b 的 Weil 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 4.5 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[18].因此,我们可以得出如下结论:

$$t_s=t_{RSA} \tag{2}$$

$$t_v=5t_{RSA} \tag{3}$$

所以,FAMIPv6 和 IBS-FAMIPv6 所需的总切换延时由式(4)、式(5)给出:

$$T_{FAMIPv6}=4a+3b+d+14t_p+t_{RSA}+4c \tag{4}$$

$$T_{IBS\text{-}FAMIPv6}=2a+2b+d+8t_p+2t_s+\max(t_v,2c+t_p) \tag{5}$$

假设访问网络与家乡网络之间的传输延时 ξ 服从 $[b,H]$ 上的均匀分布,$t_v>t_p$,令 $E(\theta)$ 和 $E(\delta)$ 分别表示 $T_{FAMIPv6}$ 和 $T_{IBS\text{-}FAMIPv6}$ 的数学期望,则

$$E(\theta)=4a+5b+d+14t_p+t_{RSA}+2H \tag{6}$$

下面计算 $E(\delta)$.令 $\delta_1=\max(t_v,2\xi+t_p)$, $\eta=2\xi+t_p$, $f_\eta(y)$ 和 $f_\xi(y)$ 分别表示 η 和 ξ 的密度函数.

当 $t_v<2H+t_p$, $f_\eta(y)=\frac{1}{2}f_\xi\left(\frac{y-t_p}{2}\right)=\frac{1}{2(H-b)}$, $t_p+2b\le y\le 2H+t_p$,

$$\begin{aligned}E(\delta_1)&=\int_{\delta_1\le t_v}\delta_1 dP(\delta_1\le t_v)+\int_{\delta_1>t_v}\delta_1 dP(\delta_1>t_v)\\&=\int_{\delta_1=t_v}\delta_1 dP(\delta_1=t_v)+\int_{\delta_1>t_v}\delta_1 dP(\delta_1>t_v)\\&=\int_{\eta\le t_v}t_v dP(\eta\le t_v)+\int_{\eta>t_v}\eta dP(\eta>t_v)\\&=\int_{t_p+2b}^{t_v}\frac{t_v}{2(H-b)}dy+\int_{t_v}^{2H+t_p}\frac{y}{2(H-b)}dy\\&=\frac{(t_v)^2+(2H+t_p)^2-2t_v\cdot t_p-2t_v\cdot 2b}{4(H-b)}.\end{aligned}$$

所以,得到

$$E(\delta_1)=\begin{cases}t_v, & t_v\ge 2H+t_p\\ \dfrac{(t_v-t_p)^2+4H^2+4H\cdot t_p-4t_v\cdot b}{4(H-b)}, & t_v<2H+t_p\end{cases},$$

$$E(\delta)=2a+2b+d+8t_p+2t_s+E(\delta_1) \tag{7}$$

为了具体分析 FAMIPv6 和 IBS-FAMIPv6 之间的性能,我们定义模型中的具体参数值:a=4ms,$b=d$=2ms,

t_p=0.5ms,因为 $t_{RSA}=t_s$,$t_v=5t_s$,最后得到两者的数学期望为

$$E(\theta)=35+t_s+2H \tag{8}$$

$$E(\delta)=\begin{cases}18+7t_s, & H\le\dfrac{5t_s-0.5}{2}\\ 20.5+2t_s+H+\dfrac{25t_s^2-45t_s+20.25}{4(H-2)}, & H>\dfrac{5t_s-0.5}{2}\end{cases} \tag{9}$$

图 7、图 8 分别给出了取定 t_s=8ms 和 H=20ms 时的总切换延时数学期望分布图.从图 7 可以看出:当签名验证算法的本机处理时间确定时,随着 H 的增大,FAMIPv6 的总切换延时的增长幅度大于 IBS-FAMIPv6;当 H 足够大时,FAMIPv6 的增长幅度约为 IBS-FAMIPv6 的两倍.因此,当访问网络远离家乡网络时,本文提出的快速认证机制能够显著降低移动 IPv6 网络总的移动切换延时.

同样地,当访问网络与家乡网络的传输延时确定时,随着 t_s 的增大,IBS-FAMIPv6 的总切换延时的增长幅度大于 FAMIPv6.而 t_s 的大小与节点处理能力(CPU 大小,内存大小等)相关,即随着计算机工艺的发展,节点处理能力的增长,签名验证算法的本机处理时间必然会下降;而 IBS-FAMIPv6 的总切换延时的下降幅度远大于 FAMIPv6.因此,当节点处理能力不断提升时,采用本文提出的快速认证机制的移动切换延时下降得更快(如图 8 所示).另外,由于本文采用的 Weil 对运算相对繁琐,若采用效率更高的 Tate 对[17,19],则将进一步降低总切换延时.

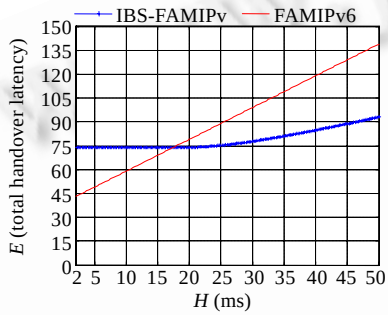


Fig.7 Expectation of total handover latency when t_s=8ms

图 7 总切换延时的数学期望分布(t_s=8ms)

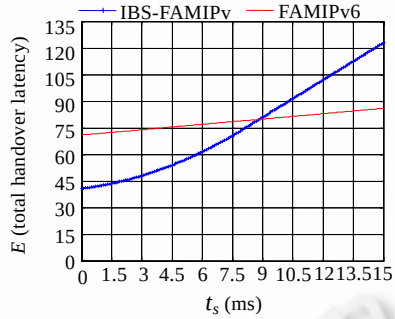


Fig.8 Expectation of total handover latency when H=20ms

图 8 总切换延时的数学期望分布(H=20ms)

4 结束语

本文提出了一种移动 IPv6 网络的快速认证机制.该机制通过采用 IBS 技术替代了传统的基于公钥证书的方式,实现了网络与用户的双向认证.通过采用 NAI 作为每个节点的公钥,极大地降低了管理密钥给每个节点带来的负担.与传统的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,本文提出的机制结合了切换和认证过程,利用 IBS 的特点,减少了访问网络与家乡网络之间的消息传输.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,虽然实现了接入认证,却忽略了数据机密性保护.但是,我们通过采用基于身份的签密机制[20],可以实现 MN 与 AR 或 MN 与 AAAv 之间的密文传输.另外,与 PKI 机制中 CA(certificate authority)的私钥保存一样,IBS 机制中系统私钥 s 的保存也是难点.我们可以采用门限思想[21]将系统私钥分发到多个不同站点共同维护.若要解决上述两个问题,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.

References:

[1] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. IETF RFC 3775, 2004.

[2] Koodli R. Fast handovers for mobile IPv6. IETF RFC 4068, 2005.
[3] Le F, Patil B, Perkins CE, Faccin S. Diameter mobile IPv6 application. Internet IETF Draft, draft-le-aaa-diameter-mobileipv6-04, 2004.
[4] Pack S, Choi Y. Pre-Authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model. In: Proc. of the IFIP TC6/WG6.8 Working Conf. on Personal Wireless Communications 2002.
[5] Kim C, Kim YS, Huh EN, Mun Y. Performance improvement in mobile IPv6 using AAA and fast handoff. In: Proc. of the ICCSA 2004. LNCS 3043, Springer-Verlag, 2004. 738−745.
[6] Eronen P, Hiller T, Zorn G. Diameter extensible authentication protocol (EAP) application. IETF RFC 4072, 2005.
[7] Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible authentication protocol (EAP). RFC 3748, 2004.
[8] Aboba B, Simon D. PPP EAP TLS authentication protocol. RFC 2716, 1999.
[9] Palekar A, Simon D, Salowey J, Zhou H, Zorn G, Josefsson S. Protected EAP protocol (PEAP) version 2. Internet IETF Draft draft-josefsson-pppext-eap-tls-eap-10, 2004.
[10] Lee BG, Kim HG, Sohn SW, Park KH. Concatenated wireless roaming security association and authentication protocol using ID-based cryptography. In: Proc. of the IEEE VTC 2003-Spring, the 57th IEEE Semiannual, Vol 3. 2003. 1507−1511.
[11] Shamir A. Identity-Base cryptosystems and signature schemes. In: Advances in Cryptology — Crypto'84. LNCS 196, Springer-Verlag, 1984. 47−53.
[12] Boneh D, Franklin M. Identity based encryption from the Weil pairings. In: Advances in Cryptology—Crypto 2001. LNCS 2139, Springer-Verlag, 2001. 213−229.
[13] Hess F. Efficient identity based signature scheme based on pairings. In: Select Areas in Cryptography—SAC 2002. LNCS 2595, Springer-Verlag, 2003. 310−324.
[14] Cha JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. In: Proc. of the Public Key Cryptography—PKC 2003. LNCS 2567, Springer-Verlag, 2003. 18−30.
[15] Yi X. An identity-based signature scheme from the Weil pairing. IEEE Communications Letters, 2003,7(2):76−78.
[16] Dupont F, Bretagne E, Bournelle J. AAA for mobile IPv6. Internet IETF Draft draft-dupont-mipv6-aaa-01, 2001.
[17] Barreto PSL, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. In: Advances in Cryptology—Crypto 2002. LNCS 2442, Springer-Verlag, 2002. 354−368.
[18] Scott M. Multiprecision integer and rational arithmetic C/C++ library (MIRACL). 2005. http://indigo.ie/~mscott/
[19] Galbraith SD, Harrison K, Soldera D. Implementing the Tate pairing. In: Proc. of the Algorithm Number Theory Symp.—ANTS V. LNCS 2369, Springer-Verlag, 2002. 324−337.
[20] Libert B, Quisquater JJ. A new identity based signcryption scheme from pairings. In: Proc. of the IEEE Information Theory Workshop (ITW 2003). 2003. 155−158.
[21] Gemmell PS. An introduction to threshold cryptography. CryptoBytes, 1997,2(3):7−12.

田野(1979－),男,重庆涪陵人,博士,主要研究领域为下一代互联网,无线移动网络安全.

张玉军(1976－),男,博士,副研究员,主要研究领域为下一代互联网,移动计算.

刘莹(1978－),女,博士生,主要研究领域为计算机系统的性能评测,网络性能评测,数据密集性大规模系统的性能评测.

李忠诚(1962－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为计算机网络,可信计算.