摘 要

移动 IP 技术是新一代移动通信发展的产物. 移动 IP 技术是指移动用户在基于 TCP/IP 的网络中移动时，不需要修改计算机原有的 IP 地址，仍能继续享有原网络中一切权限和服务的技术. 其主要目的是无论接连在本地链路还是移动到外地网络，移动节点总是通过本地地址寻址.

作为移动 IP 中几个关键技术之一，移动 IP 快速切换对于提高网络服务质量起着至关重要的作用. 移动 IP 快速切换的实现将会使移动通信中更多的潜在服务项目成为现实，从而满足人们随时随地通信的需求. 相比有线网络，无线通信有着更多的安全风险. 本文在对移动 IP 切换技术经过系统研究后，提出了两个安全协议. 协议既满足了安全性要求，又提高了切换效率.

作者在本文中主要取得的研究结果如下：

(1) 提出一种新的基于身份移动 IP 注册协议. 移动节点和家乡代理通过对方公钥、自身私钥、随机参数以及系统参数来计算双方的共享密钥. 这种新的方案利用双线性对的性质，不仅能有效地验证双方的身份，而且移动节点不需要进行复杂的双线性对计算. 该协议很好的解决了密钥协商和密钥更新等问题. 最后对协议的安全性和效率进行了分析.

(2) 提出了一种新的移动 IP 切换技术. 网络结构与层次化移动 IP 类似，移动锚点增加了组播路由的功能. 移动节点的组播地址取代本地转交地址，从而减小移动节点在域内切换的延时. 节点的接入认证采用改进的 2 层身份签名算法. 分析表明，协议在实现双向认证的前提下切换效率也得到了显著的提高.

关键词：基于身份密码学　注册协议　2层身份签名　切换技术

Abstract

Mobile IP, which is the product of the new generation mobile communication, is a kind of technology that mobile users still can continue to enjoy all of the original network services and rights when they roaming across the network based on TCP/IP, with not using to modify the computer original IP address. Its main purpose is that the mobile node always select routing through local address whether one in local link or not.

As one of the several key technologies of mobile IP network, to quickly switch plays an vital role in improving the service quality. Mobile IP fast switching will make more potential services in mobile communication become a reality, and satisfy the users to communicate in anytime and anywhere. Compared with cable network, wireless communication has more safety risk. As the result of the system research in mobile IP switching technology, two security agreements are proposed, which not only satisfy safety requirements but also be improved in efficiency.

The main contributions of the dissertation are listed as follows.

(1) A new identity-based mobile IP registration protocol is proposed. The mobile node and its home agent calculate their shared key separately through each others' public key, the private key, random parameters and the system parameters. The new protocol utilizes the nature of bilinearity not only to verify the identity between the mobile node and its agents, but also for the mobile node to prevent the complicated bilinear pairing computations. The protocol resolve the issues of dynamic key agreement and update efficiently.

(2) A new mobile IP switching technology is proposed. The mechanism which has the same network structure with the hierarchical mobile IP, adds the function of multicast routing to mobile anchor points. The multicast address is instead of the local care of address, thus the switching delay within the domain decreased. Node access authentication use the modified 2-hierarchical identity signature algorithm. Analysis shows that the scheme realizes two-way authentication while the switching efficiency also got a great improvement.

Keyword: Identity-based cryptography Registration protocol 2-Hierarchical identity signature algorithm Handoff

目 录

第一章 绪 论

移动 IP 协议[1-4]是在 IP 协议的基础上，为了支持节点移动性而提出的网络层解决方案——一种特殊的路由机制. 移动 IP 协议的主要设计目的是，移动节点在改变网络接入点时，不需要改变其 IP 地址，且能够保持移动过程中通信的连续性. 本章首先介绍了移动 IP 技术发展的历史背景，应用前景和研究的现实意义. 接下来，对国内外该领域的研究做了简单的介绍. 最后是本论文的研究成果和章节安排.

1.1 移动 IP 技术的产生及应用前景

1.1.1 移动 IP 技术的产生

在二十一世纪的今天，信息科学发展突飞猛进，使人们的生活发生了巨大的改变. 互联网技术和移动通信技术更是不断地深入我们生活的各个角落. 随着这两种信息技术的应用更加广泛和深入，人们越来越迫切地需要一种移动互联网技术能够让我们随时随地接入互联网，并且得到各种各样便捷的服务.

目前互联网中普遍使用的 IP 协议，要求每个主机都有一个 IP 地址. 而这个 IP 地址不仅能够标志一个主机，它的网络前缀同时表示了主机所在的物理网络位置. IP 协议正是通过这种寻址方式来进行路由发包，从而使两个通信对端能够通信. 可是当主机移动到其他网络中时，IP 地址的网络前缀就不能正确的表示其所在的网络位置，进而也不能正确的路由发包. 为了让移动主机能够接入互联网，目前提出以下三种解决方案：移动节点改变位置的同时改变 IP 地址、根据特定的主机地址进行路由选择，以及在链路层采用蜂窝数字分组数据.

首先讨论第一种方案的可行性. 采用网络前缀路由要求同一条链路上所有节点的 IP 地址具有相同的网络前缀. 因此，当一个节点从一条链路切换到另一条链路上时，为了体现新链路的网络前缀，节点至少应该改变它的 IP 地址的网络前缀部分，但它可以保留 IP 地址的主机部分，只要新链路上没有别的节点使用相同的主机部分就可以，否则只能改变整个 IP 地址了. 一旦节点改变了 IP 地址，它就可以通过新链路利用新地址进行以后的通信了. 然后 IPv4 有一个非常不好的约定，即 TCP 连接两端的 IP 和端口是保持不变的. 当目标节点的 IP 地址发生变化时，这个约定将断开连接. 所以移动节点改变 IP 地址时，两个节点之间正在进行的通信会中断，只能再由移动节点以新的 IP 地址建立一条新连接. 这样，从节点的可

移动性的定义来看，当节点移动时只改变它的地址不能解决移动性问题.

对于特定主机路由方案，要想实现节点的移动性，必须至少向从移动节点的家乡链路到外地链路沿途的所有节点传送特定主机路由．每次节点切换路由时，上面那些路由中的一部分必须进行更新．然而在全面解决互联网移动性的将来，需要传送特定主机路由的数目将会呈指数增长，不具有实际可操作性．同时，采用特定主机路由的方案存在可扩展性差、可靠性低和安全隐患大等问题.

蜂窝数字分组技术虽然能支持多种协议，可是它需要大量的管理维护以及新的网络基础设施，和现有的互联网无法兼容.

移动 IP 技术是网络层支持主机移动的解决方案，它不涉及互联网协议的其他层．移动 IP 是通过在节点中建立路由表，实现转发数据到外地链路的移动主机上．移动 IP 技术不仅能支持移动主机在不同网段间的移动，也能支持其在不同网络，不同介质间移动时的通信.

1.1.2 移动 IP 技术的应用前景

移动 IP 技术只是网络层的移动解决方案，它与应用在什么媒介上毫无关系，与底层的链路特性亦无关．正因为这样的特性，它能够实现移动主机在不同介质间的移动，并且不会出现切换时中断的现象．这正是蜂窝式数字分组数据和 802.11 技术所不能做到的．而移动 IP 技术正因为同时具有同质移动和异质移动的功能，再加上全 IP 网络大势所趋，所以它已经成为未来移动通信网络的标准.

移动 IP 提供了一种路由机制，使移动节点可以用一个永久的 IP 地址连接在任何链路上．也就是说，移动主机无论连接到哪个数据链路层的接入点，都应该能用原来的 IP 地址通信．同时，移动 IP 的设计标准要求具有移动能力的节点应该可以和不具备移动 IP 功能的节点通信．事实上，我们只是在网络中某些特定节点中增加了某些功能以支持移动主机的移动功能，而对于网络中的其他节点来讲是透明的，更不会影响网络中的其他结构.

移动 IP 设计标准同时规定，移动节点不能比网络中的其他非移动节点具有更多的安全风险.

综合以上的几点，我们可以看出移动 IP 解决方案具有可扩展性良好、可靠性强和安全性高等特点．它必然将成为未来发展“移动互联网”的关键技术.

1.2 国内外研究概况

1994 年 A.Myles 和 C.Perking 总结了先前的两种移动主机协议，提出了一种新的协议，即移动 IP 协议的前身．1996 年，IETF 发布移动 IP 协议标准(草案)之后，移动 IP 技术正式进入了快速发展的时期．协议标准(草案)包括 RFC2002[5]、

RFC2003[6]、RFC2004[7]、RFC2005[8]和 RFC2006. 其中 RFC2002 定义了移动 IP 协议、IP 移动性支持，RFC2003、RFC2004 和 RFC1701 分别定义了移动 IP 的三种隧道技术：IP-in-IP 隧道封装、IP 的最小封装和通用路由封装. RFC2005 叙述了移动 IP 的应用. RFC2006 定义了移动 IP 的管理信息库 MIB.

对于移动 IP 协议的注册过程，目前已公开提出的移动 IP 注册协议大体上分为三类[9]：一是采用对称密码体制来实现移动实体之间的相互认证；二是采用基于证书的公钥密码体制来完成移动实体之间的相互认证；三是采用对称密码体制和公钥密码体制(包括基于证书的公钥密码体制和基于身份的公钥密码体制)相结合的方案来实现移动实体之间的相互认证.

在 RFC2002、RFC3220[10]、RFC3344[11]中提出的移动 IP 注册协议[5,10-11]采用手动分发对称密钥给三个移动实体来完成相互认证. 在拥有少量移动用户和小型规模的移动网络中，这种方案的注册协议性能非常良好，并且对称密钥加解密运算所占资源和耗时都非常少，注册时延短. 然而，当移动网络的规模急剧增大时，保密通信前手动分发密钥，这对相距较远的用户将需要很大的代价[12]；而且为了使 n 个用户之间进行保密通信，将需要对所有用户两两分发密钥，当 n 不断增大时，代价是非常大的. 所以，它的缺点就是不便于密钥管理，网络扩展性不好.

为了适应大规模网络中移动用户的需求，文献[13-15]提出了通过采用基于证书的公钥密码体制来实现三个移动实体之间的相互认证的方案. 该方案的优点就是便于密钥管理、扩展性很好、安全性保证完备. 但缺点是，移动用户端的计算能力、存储空间以及电池储蓄量等都很有限，在移动用户端进行公钥加解密运算和基于证书的一系列操作，将会大大影响移动 IP 注册协议的性能，使得注册时延变长. 尽管目前提出很多此类方法的改进方案[16-17]，但由于这种方案的缺点大大影响了移动 IP 注册协议的性能，所以通常不适合在实际中应用.

在考虑到以上两种方案的缺点之后，人们开始着眼于用对称密码体制和公钥密码体制相结合的方案[18-22]来改善移动 IP 注册协议的性能. 该方案融合了对称密码体制运算量小的优点以及基于证书的公钥密码体制网络扩展性好的优点. 首先，在移动用户和家乡代理之间采用对称密码体制或者基于身份的密码体制[23]来进行两者之间的相互认证，克服了移动用户端计算能力有限的缺点. 其次，在外地代理和家乡代理之间仍然采用基于证书的公钥密码体制，使得注册协议仍然便于在大型网络中应用. 这种移动 IP 注册协议与只采用公钥密码体制的注册协议相比，网络扩展性一样好，但是大大降低了注册时延，改善了移动 IP 注册协议的性能，并且更具有使用价值.

由于移动 IP 协议不支持快速切换，目前针对各种网络环境中的需求提出了很多切换方案[24-25]. 总的来说，包括基于微移动的切换技术、基于暗示的切换技术、基于链路层的切换技术、基于组播的切换技术和基于位置的切换技术等类别. 2005

年 8 月 IETF 发布了 RFC5380[26]，提出了层次化移动切换技术，引入了移动锚点的概念来减少移动节点切换时的信令数量和传输延时．2005 年 7 月 IETF 发布了 RFC4068[27]，提出了快速切换技术，该技术旨在快速重建路由，使得切换过程中发往旧的转交地址的数据包能够被路由到新的转交地址．目前，就这两种技术也提出了很多改进以及融合的技术[28-29]．关于这两种方案的具体内容我们将在第四章做以概述．

1.3 论文的主要工作和章节结构

1.3.1 主要工作

论文的主要工作包括：

• 设计了一种新的基于身份移动 IP 注册协议．

根据双线性对的性质，提出一种密钥协商方案．利用该方案，提出一种完整的双向认证过程，并设计出一种新的移动 IP 注册协议．最后对该协议进行了安全性分析和效率分析．

• 设计了一种新的基于组播层次化移动 IPv6 切换技术．

分析了田等人提出的 2 层身份签名机制[30]，通过改进得到一种能够提供私钥对父亲节点也能保密的方案，同时该方案亦能减小签名验证时节点的计算量．应用上述方案提出一种基于组播的层次化移动 IPv6 切换技术．最后分析新协议的安全性和切换延时．

1.3.2 章节安排

本论文共分为五章，具体安排如下：

第一章　介绍了移动 IP 技术产生的背景和意义，回顾了目前在注册协议和切换技术方面的研究现状．最后简述了论文的主要贡献及章节安排．

第二章　介绍本文所需要的一些预备知识，包括基于身份密码学的数学基础——椭圆曲线理论、双线性对，以及密码学方面的介绍，包括基于身份密码学，Diffie-Hellman 算法，哈希函数等．最后对移动 IP 的基本原理做了简述．

第三章　对注册消息及其安全性做了介绍，基于双线性对的性质，提出了一种高效的基于身份移动 IP 注册协议，并对其安全性和效率做了分析．

第四章　对层次化移动 IPv6 的原理做了介绍，对于田等人提出的 2 层身份认证方案做了改进，并在此基础上提出了一种基于组播的层次化移动 IPv6 切换技术．最后，对方案的安全性和效率做了分析．

第五章　总结了全文，并指出了以后的研究方向．

第二章 预备知识

移动IP是下一代通信网络中的重要课题，在开始介绍本文的研究成果之前，有必要对所需的基础知识进行简要介绍. 本章首先介绍了有限域上椭圆曲线以及双线性对的概念，后两章中所提出协议的安全性保证就是利用了双线性对的性质；接着我们介绍了协议所用到的密码学知识，包括基于身份密码学、Diffie-Hellman算法和哈希函数等；最后概述了移动IP协议. 这些知识是我们后续研究工作的基础.

2.1 数学基础

2.1.1 有限域上的椭圆曲线理论

定义2.1 设G是一个非空集合，在G内定义了一种代数运算"$\cdot$"，满足以下性质：

- 封闭性：对任意的a、$b\in G$，恒有$a\cdot b\in G$；
- 结合律：对任意的a、b、$c\in G$，恒有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$；
- G中有一单位元e存在，对任意的$a\in G$，恒有$a\cdot e=e\cdot a=a$；
- 对任意的$a\in G$，存在a的逆元$a^{-1}\in G$，使得$a\cdot a^{-1}=a^{-1}\cdot a=e$；

则称G对于"$\cdot$"运算构成一个群.

若群G中，对任何a，$b\in G$，恒有$a\cdot b=b\cdot a$，则称G为交换群，也叫Abel群. 元素个数有限的群称为有限群，元素的个数称为该有限群的阶. 若一个群G的每一个元素都是G的某一个固定元a的乘方，就称G为循环群，称a是G的生成元.

定义2.2 设S是一个非空集合，若在S中定义了加法"+"和乘法"$\cdot$"两种运算，且满足下述性质：

- S关于加法运算构成Abel群，其加法单位元记为0；
- S中所有非零元关于乘法运算构成Abel群，其乘法单位元记为1；
- 对任意a，b，$c\in S$，加法和乘法间存在如下分配律：

$$a\cdot(b+c)=a\cdot b+a\cdot c \tag{2-1}$$

$$(b+c)\cdot a=b\cdot a+c\cdot a \tag{2-2}$$

则称S关于加法"+"和乘法"$\cdot$"构成一个域.

由有限个元素所构成的域称为有限域，也叫伽罗瓦域．域中元素的个数称为该有限域的阶．有限域的阶一定是一个素数 p 的幂 p^n，n 为正整数，有限域则记为 $GF(p^n)$.

定义 2.3 设 p 为一素数，n 为正整数，$q=p^n$．而 $GF(q)$ 是 q 个元素的有限域，记 $GF(q)$ 的代数闭包为 $\overline{GF(q)}$．$GF(q)$ 上的 Weierstrass 方程

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, a_i\in GF(q)$$

决定仿射平面 $A^2(\overline{GF(q)})$ 上的一条曲线．添加上无穷远点后，就得到射影平面 $P^2(\overline{GF(q)})$ 上的一条曲线 E，若曲线 E 是非奇异的，则 E 称为有限域 $GF(q)$ 上的一条椭圆曲线.

可以证明 E 是一条椭圆曲线，当且仅当判别式 $\Delta\neq 0$．其中，

$\Delta=-b_2^2b_8-8b_4^3-27b_8^2+9b_2b_4b_6$，

$b_2=a_1^2+4a_2$，

$b_4=2a_4+a_1a_3$，

$b_6=a_3^2+4a_6$，

$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$.

从几何角度利用弦切法可以在 $E(GF(q))$ 上定义“+”运算：对于椭圆曲线上的点 P，Q，过点 P，Q 的直线(若 $P=Q$，则取过点 P 的切线)和椭圆曲线必有第三个交点(考虑重数)，过该点和O的直线与椭圆曲线的另一交点即定义为 $P+Q$.

定义 2.4 设 E 为椭圆曲线，m 为正整数．定义 $E[m]=\{P\in E(\overline{GF(q)})|[m]P=\mathrm{O}\}$，即 $E[m]=Ker[m]$.

定义 2.5 设 $P\in E[m]$(P 与 Q 可以相同)，对任一 $X\in E$，

$g(X+P)^m=f([m]X+[m]P)=f([m]X)=g(X)^m$.

故 $e_m(P,Q)=g(X+P)/g(X)$ 是一个 m 次单位根($\overline{GF(q)}(E)$ 中的任一函数或常数，所以 $e_m(P,Q)$ 是一个常数)．g 的取法可以差一个常数因子，但这不影响 $e_m(P,Q)$ 的值，故得到

$e_m: E[m]\times E[m]\to\mu_m$，

μ_m 为 m 次单位根组成的群，e_m 称为 Weil 对.

Weil 对具有以下性质：

• 双线性性：对任意 P_1、P_2、$Q\in E[m]$，有 $e_m(P_1+P_2,Q)=e_m(P_1,Q)e_m(P_2,Q)$.

• 恒等性：对任意 $P\in E[m]$，有 $e_m(P,P)=1$.

• 交错性：对任意 P、$Q\in E[m]$，有 $e_m(P,Q)=e_m(Q,P)^{-1}$.

• 非退化性：对任意 $P\in E[m]$，有 $e_m(P,Q)=1\Leftrightarrow Q=O$.

• 相容性：设 α 是一个非零自同态，则 $e_m(\alpha(P),\alpha(Q))=e_m(P,Q)^{\deg\alpha}$.

定义 2.6 设 G_1，G_2 分别为 q 阶的加法群和乘法群，P 为 G_1 的生成元，假设 $\hat{e}:G_1\times G_1\to G_2$ 为满足以下性质的双线性映射[31]：

• 双线性性：对所有的 P、$Q\in G_1$，a、$b\in Z_q^*$ 都有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$.

• 非退化性：对生成元 P，有 $\hat{e}(P,P)\neq 1$.

• 可计算性：对所有的 P、$Q\in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$.

这样的双线性对可以通过椭圆曲线中 Weil 对(或 Tate 对)来实现.

2.1.2 数学难题——DH 问题

定义 2.7 CDH 问题(Computational Diffie-Hellman Problem). 对于给定的(P，aP,bP)，其中 $a,b\in Z_q^*$，输出 abP.

定义 2.8 APCDH 问题(Add-Point Computational Diffie-Hellman Problem). 对于给定的(P,aP,bP,cP,dP)，其中 $a,b,c,d\in Z_q^*$，输出 $acP+bdP$.

定理 2.1 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，aP,cP)，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.

2.2 密码学基础

2.2.1 基于身份密码学

公钥证书基础设施的体系中，通常通过公钥证书来实现公钥与实体的身份关联．然而这种方式的证书管理过程需要很高的计算开销和存储开销，同时由于公钥生成的随机性，实体公钥与身份的不对应给公私钥及实体身份的管理带来了沉重的负担．

1984 年，Shamir 提出了一种公钥密码体制[32]，该体制能大大减小公钥系统的复杂度．它选择任意比特串作为公钥，由私钥生成中心生成对应的私钥．通常选用用户身份作为公钥，因此叫做基于身份的公钥密码学(IBC)．

基于身份密码体制最大的优势就在于它简化了传统基于证书的公钥体制负担最重的密钥管理过程．一般而言，基于身份密码系统拥有如下特点：用户公钥是他的身份信息(或者是从身份信息变化而来)；不需要公钥目录；消息加密或签名验证过程只需要接受者或签名者的身份信息加上一些系统参数．

因此，基于身份密码体制在密钥分发等方面远优于基于证书的公钥系统，它只需维护私钥生成中心(PKG)产生的公开系统参数，这个开销将远低于维护所有用户的公钥所需的开销．

2.2.2 身份签名机制

身份密码学技术是在超奇异椭圆曲线上基于双线性对实现的，下面首先介绍身份签名机制中需要用到的 PKG 公开参数．随机选择两素数 p、q，满足 $p=2 \bmod 3$ 和 $p=6q+1$．设 E 为 F_q 上的超奇异椭圆曲线．有理数点 $E(F_q)=\{(x,y)\in F_q\times F_q:(x,y)\in E\}$ 形成阶为 $p+1$ 的循环群．设 $(G_1,\cdot)$ 是阶为 q 的循环子群，$P\in G_1$ 的生成元，$(G_2,\cdot)$ 是 $F_{p^2}^*$ 中所有阶为 q 的元素组成的子群．双线性对就是 $\hat{e}:G_1\times G_1\to G_2$．

身份签名机制(IBS)主要由四个阶段组成，即参数生成阶段、密钥生成阶段、签名阶段和验证阶段．私钥生成中心在参数生成阶段初始化系统，生成系统参数并公开，保存主密钥 s，主密钥 s 用于密钥生成阶段为系统用户计算私钥，拥有某个身份 ID 的签名者用私钥生成中心为他生成的私钥在签名阶段对某个消息签名，而验证者则用该身份 ID 在验证阶段对签名进行验证．

在移动 IP 网络中，移动终端的计算能力有限，在设计签名机制时应尽可能减

少移动终端的计算复杂度，将签名机制中复杂的计算过程放在验证阶段.

2.2.3 Diffie-Hellman 密钥交换算法

Diffie-Hellman 密钥交换算法[33]用于建立共享密钥. 它可以使远程通信各方无需安全信道就能实现相互交换密钥. 它的安全性是基于有限域上的离散对数问题.

其具体方法如下：Alice 和 Bob 选择并公开一组系统参数(F_q，q，E，P，n). 其中，F_q 为有限域. p 为大素数，$q \in \{p, 2^m\}$即该有限域为素域或者有限域的阶是 2 的幂次. E 是有限域 F_q 上的安全椭圆曲线群，$P \in E(F_q)$是 E 上某个阶为大素数 n 的点. Alice 和 Bob 可以通过如下的交换过程建立相同的密钥：

• Alice 随机选取整数 $a \in Z_n$ 予以保密，并计算 $Q_a = aP$；

• Bob 随机选取整数 $b \in Z_n$ 予以保密，并计算 $Q_b = bP$；

• Alice 将 Q_a 传送给 Bob，而 Bob 将 Q_b 传送给 Alice；

• Alice 收到 Q_b 后，计算 $k = a(Q_b) = abP$；Bob 收到 Q_a 后，计算 $k = b(Q_a) = baP = abP$；则 k 就可作为 Alice 和 Bob 所使用对称密码体制中的密钥.

如果攻击者可以窃听，则他知道 P，Q_a，Q_b，为了获得密钥 k，攻击者必须由 P，$Q_a = aP$，$Q_b = bP$ 求得 $k = abP$，这是椭圆曲线 CDH 问题. 如果椭圆曲线离散对数问题可解，即对于输入 Q，存在多项式时间的算法求得 k，使得 $Q = kP$，则椭圆曲线 CDH 问题可解. 其逆命题是否成立目前仍是一个公开的问题.

2.2.4 哈希函数

哈希(Hash)函数[12,34]也称为杂凑函数，它将任意长度的输入消息串变换成为固定长度的输出串，这个输出串称为该消息的哈希值(也称杂凑值). 下面给出哈希函数的定义.

定义 2.1 称函数 $y = h(x)$是一个 Hash 函数，如果它满足以下条件：

• 输入的 x 的长度是任意的，输出的 y 的长度是固定的；

• 对于给定的输入 x，计算输出的 Hash 值 y 容易；反过来，对于给定的 Hash 值 y，找出输入 x，使得 $y = h(x)$在计算上不可行；

• 找出两个不同的输入 x 和 x'，即 $x \neq x'$，使得 $h(x) = h(x')$在计算上不可行；给定一个输入 x，找出另一个不同的输入 x'，即 $x \neq x'$，使得 $h(x) = h(x')$在计算上

不可行.

哈希函数可以按其是否有密钥控制划分为两大类：一类是有密钥控制，以 $h(k,M)$ 表示，为密码哈希函数；另一类无密钥控制，为一般哈希函数. 无密钥控制的单向哈希函数，其哈希值只是输入字串的函数，任何人都可以计算，因而不具有身份认证功能，只用于检测接受数据的完整性. 而有密钥控制的单向哈希函数，要满足各种安全性要求，其哈希值也称为认证码.

一般哈希函数通常被应用于保证数据完整性，步骤如下. 在 T_1 时刻计算特定消息 x 的哈希值，以某种方式保护哈希值的完整性. 在随后的 T_2 时刻，执行下列测试确定消息是否被修改，即消息 x' 是否与源消息相同. 计算 x' 的哈希值并与保护的哈希值进行比较：假如两者相等，就认为输入也是相等的，消息也就未被修改. 保护一个大消息的完整性问题就简化为保护一个小的固定大小的杂凑值. 哈希函数和数字签名方案一起应用于数据完整性. 由于某种原因，消息通常先进行杂凑，哈希值作为消息的表示代替原消息进行签名.

密码哈希函数在实际中有广泛的应用，在密码学和数据安全技术中，它是实现有效、安全可靠数字签名和认证的重要工具，是安全认证协议中的重要模块. 由于密码哈希函数应用的多样性和其本身的特点而有很多不同的名字，其含义也有差别，如压缩函数、紧缩函数、数据认证码、消息摘要、数字指纹、数据完整性校验、密码检验和、消息认证码(MAC)、篡改检测码(MDC)等.

2.3 移动 IP 协议概述

目前移动 IP 有两个版本：移动 IPv4 和移动 IPv6[35]. 移动 IPv4 是为了与当前的 IPv4 网络兼容而提出的，移动 IPv6 是为了适应未来的 IPv6 网络而提出的.

2.3.1 移动 IPv4

(1) 移动 IPv4 的功能实体及其他常用术语

• 移动节点(MN)：在不同网络或者子网链路中切换的移动主机或者路由器.

• 家乡代理(HA)：位于移动节点家乡链路上的路由器. 其主要功能：负责把发往移动节点的分组通过隧道转发给移动节点，维护移动节点当前位置等信息.

• 外地代理(FA)：位于移动节点所访问的外地链路上的路由器. 其主要功能：

对于发往移动节点的报文，外地代理通过与其家乡代理之间的隧道接收并转发给移动节点；对于从移动节点发出的报文，其服务与其他 IP 网络相同.

• 对端节点(CN)：与移动节点通信的对等实体.

• 家乡地址(HoA)：移动节点在家乡链路中拥有的 IP 地址.

• 转交地址(CoA)：移动节点在外地链路中的临时 IP 地址.

• 代理通告：移动代理周期性地在本链路发布的通告消息，以告知移动节点所处的链路信息、网络地址等信息.

• 移动绑定：家乡地址和转交地址的关联信息.

• 隧道技术：一种数据分组被封装在另一数据分组的净荷中进行传送的技术.

(2) 基本框架

在移动 IPv4 中，移动节点通过使用一对 IP 地址实现移动功能. 当连接到外地网络时，移动节点从外地代理处获得或者通过自动配置的方式获得一个临时转交地址. 通过位置注册，移动节点将转交地址报告给家乡代理. 在获知移动节点当前的外地代理信息后，通信对端节点发送来的数据包首先被路由到家乡网络，家乡代理截获该数据包并通过隧道技术将其转发到移动节点的当前位置. 由移动节点发出的数据包则直接被路由到对端节点.

(3) 基本流程

移动 IPv4 的基本流程如图 2.1 所示：

• 移动代理(HA 或者 FA)通过代理通告消息告诉 MN 移动代理的存在，MN 也可以通过当前访问网络发送代理请求获得代理通告消息. MN 收到代理通告之后，判断其所在网络是否发生变化.

• 若 MN 从外地链路返回到家乡链路，发送注册请求注销其在外地链路上的转交地址；若 MN 移动到新的外地链路，首先获得转交地址，随后发送注册请求注册转交地址. HA 将新的转交地址与其家乡地址进行移动绑定，返回注册应答消息，注册完成；另外，当 MN 在外地链路之间切换时，以及 MN 的注册消息过期时同样需要进行与上述过程相同的注册.

在移动 IPv4 中，有两种转交地址：配置转交地址和代理转交地址. 其中，配置转交地址通过 DHCP、BOOTP 等协议得到，它是一个真正独立的 IPv4 地址，此时移动节点可以自己用此地址发送或者接受数据包；代理转交地址实际上是外地代理的地址，外地代理代替移动节点接收数据包，简单处理后再把数据包传送给移动节点.

如果 MN 获得的是配置转交地址，则可以作为一个独立的节点收发数据包，

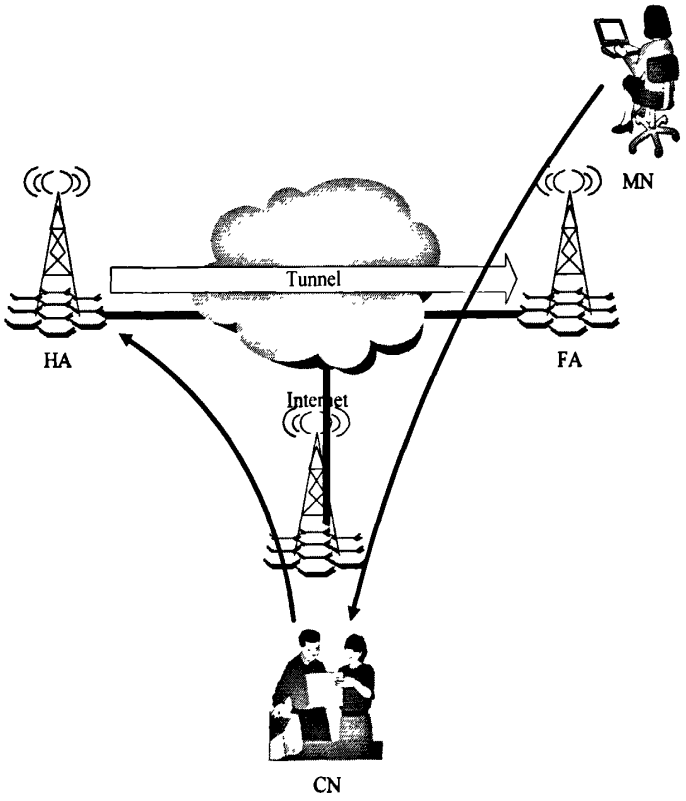

图 2.1 移动 IPv4 基本流程示意图

不需要外地代理的参与；如果 MN 获得的是代理转交地址，MN 的注册就必须借助外地代理才能完成.

•HA 截获发往 MN 家乡地址的数据分组，通过隧道技术将该数据分组发送到 MN 的转交地址. 隧道的输出端点 FA 把收到的报文进行拆封后，交给 MN. MN 发往 CN 的数据分组通过标准的 IP 路由机制发送，不通过 HA.

2.3.2 移动 IPv6

(1) 移动 IPv6 的功能实体以及概念说明

• 移动 IPv6 中涉及的功能实体主要有移动节点、家乡代理、对端节点和接入路由器. 这些功能实体的概念包括家乡地址，转交地址等术语的含义与移动 IPv4 类似.

• 移动 IPv6 没有外地代理的概念. 移动 IPv6 使用 IPv6 的特性，如邻居发现和地址自动配置等，无需外地网络上的路由器提供特别的功能支持.

• 转交地址只定义了配置转交地址一种.

• 绑定缓存：通信节点和代理维护的一种数据信息，用于记录移动节点的家乡地址和其当前转交地址之间的对应关系.

•移动 IPv6 中，除家乡代理截取的分组外，多数分组都是使用 IPv6 路由头直

接发送到移动节点，不需要使用隧道封装.

(2) 基本框架

在移动 IPv6 中，移动节点同样使用唯一的家乡地址连接到任何链路上；同时每当移动节点移动到一个新子网，它就从接入路由器获得一个临时转交地址，并且将它注册到家乡代理. 与移动 IPv4 一样，对端节点发向移动节点家乡地址的数据包会被家乡代理截获并通过隧道方式转发给 MN 的转交地址；与移动 IPv4 不同的是，移动节点能够在对端节点上注册自己的转交地址，从而实现移动节点与通信对端节点之间的直接通信.

(3) 基本流程

移动 IPv6 的基本流程如图 2.2、图 2.3 所示：

• MN 在家乡链路上有家乡地址 HoA. 当 MN 没有发生移动时，如果 CN 与 MN 通信，CN 发送的数据包会按照正常的路由方式到达 MN. MN 在切换时，首先收到包括本地链路前缀信息的代理通告消息. 收到通告消息后，根据前缀信息通过地址自动配置得到一个转交地址 CoA.

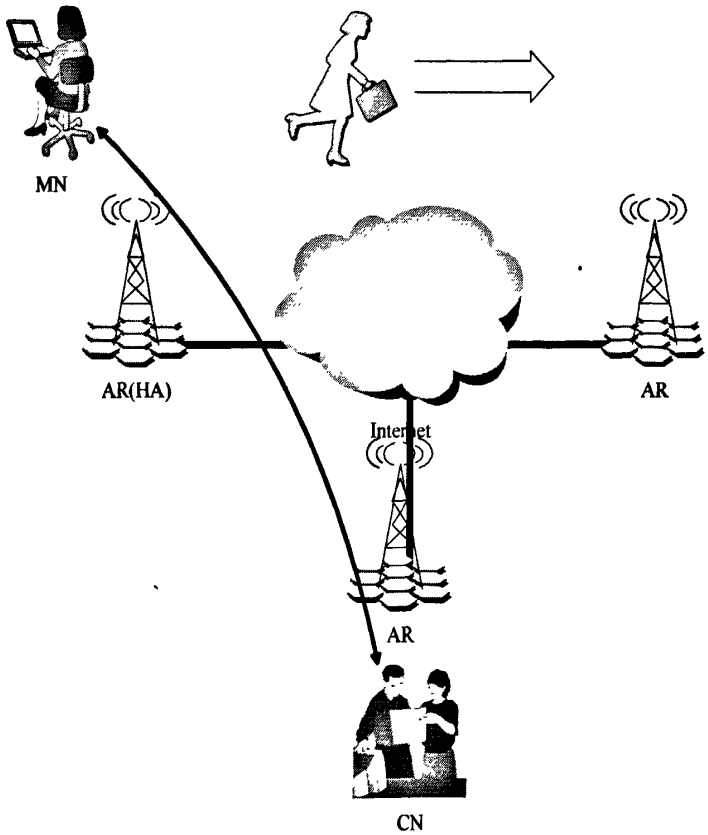

图 2.2 移动 IPv6 基本流程示意图(移动节点移动前)

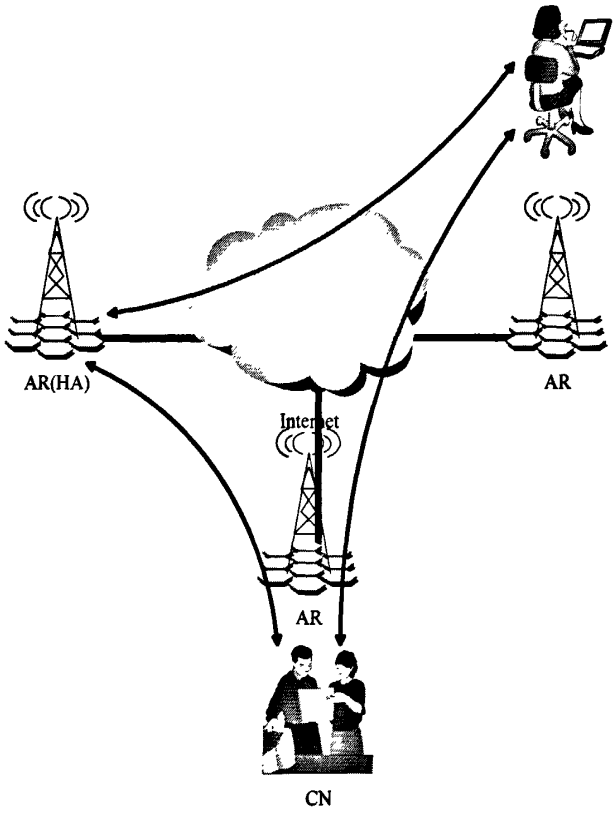

图 2.3 移动 IPv6 基本流程示意图(移动节点移动后)

• MN 发送信息给 HA，告诉它现在的转交地址 CoA. 此后，HA 再发现有需要送到 MN 的原来地址 HoA 的数据包，它会把这个数据包截获，然后把这个包作为净荷，在其上面再加上一层 IPv6 报头，把新的数据包发送到 MN 的新地址 CoA.

• MN 收到 HA 转发过来的数据包以后，通过检查数据包的内层源地址，它知道 CN 想与它进行通信，于是会发送一个绑定更新给 CN，告诉自己的新地址 CoA. 此时，对端节点就在它的绑定缓存中增加一条对应此移动节点的条目.

• CN 收到这个数据包以后，会记录下 MN 的新地址 CoA. 如果再有数据包需要发送给 MN，CN 首先会检查绑定缓存. 如果其中有对应此地址的条目，它会直接把数据包发给地址 CoA，至此 MN 和 CN 之间可以实现双向直接通信；如果没有对应其的缓存条目，则按正常方式发送.

2.4 本章小结

本章对移动 IP 协议所涉及的基本知识作了简要的介绍，包括数学基础知识(有限域上的椭圆曲线、双线性对等)、密码学基础(基于身份密码学简介、Diffie-Hellman 算法、哈希函数等)和移动 IP 协议简介. 本章的论述是后面几章对移动 IP 注册协议和切换机制进行深入研究的基础.

第三章　基于身份的移动 IP 注册协议

在一种新的密钥分配方案基础上，设计出一个高效的安全移动 IP 注册协议. 本章首先介绍了移动 IP 注册协议以及它的安全性要求，接着提出一种新的安全注册协议. 这种新的密钥协商方案利用双线性对的性质，不仅能有效地验证移动节点和代理之间的身份，而且移动节点不需要进行复杂的双线性对运算. 另外每次注册时，移动节点和代理都选取不同的随机数，从而有效地保证了安全性. 最后对安全性和效率方面作了说明.

3.1　移动 IP 注册协议

由上一章的准备知识我们知道，移动 IP 注册协议主要涉及三方，移动节点、移动节点的家乡代理和移动节点正在访问的外地代理. 移动代理之间通过有线网络连接，移动节点通过无线接入点接入网络. 当移动节点从本地网络移动到外地网络时，需要在移动节点、外地代理和家乡代理之间交换信息，注册创建或修改了一个移动绑定，并在生存期内将移动节点的家乡地址与转交地址关联起来，以实现节点通信时的移动性.

注册的主要目的是为了将移动节点的转交地址告诉家乡代理，从而家乡代理可以通过隧道将数据包发送到移动节点的转交地址. 在家乡代理处，有一张绑定对应表，这张表中的每一个绑定表项对应着一对移动节点的家乡地址和转交地址. 注册的过程实际上就是产生、修改或删除家乡代理中移动节点绑定表项的过程. 另外，每一次注册都只是在一定的生存期内有效，超过生存期时移动节点需要重新注册.

(1)　注册过程

移动节点在以下情形主动发送注册请求消息启动注册过程：检测到网络发生变化、外地代理重新启动和当前注册生存期接近超期. 移动节点离开家乡网络时所发的注册请求使家乡代理创建或是修改它的绑定. 而当它返回家乡网络时，注册请求消息使家乡代理删除它以前的所有绑定. 当注册请求发送到外地代理时，外地代理要检查注册请求消息，如果有什么不对的地方，它将抛弃这个注册请求消息并发送一个应答消息来拒绝这次注册请求；否则，它就将消息传递给移动节点的家乡代理.

收到注册请求后，家乡代理首先进行有效性检查，若注册请求有效，家乡代

理则更新移动节点绑定表项中的转交地址及生存期等信息，并向移动节点返回一个注册应答消息，告诉移动节点注册成功．若注册请求无效，家乡代理会向移动节点发送一条注册应答，并注明失败原因．此时，家乡代理不改变移动节点的绑定表项．家乡代理发送的注册应答经过的路径与激起这个应答的注册请求路径正好相反．

移动节点收到注册应答后，也需要检查应答消息的有效性．如果消息有效，那么它就检查编码域，看这次注册请求是已经被接受还是被家乡代理或者外地代理拒绝．若接受，那么移动节点不再重发注册请求，并使用注册的转交地址进行通信．若拒绝，那么移动节点修正错误后重新尝试一个注册．如果在一个正常的时间间隔内没有收到任何注册应答，移动节点可以再发送一个注册请求，并使用时间戳为每次重传选择一个新的注册标识，进行一次新的注册．如果使用了“即时”方式，那么，重传不加改变的未应答请求．这样发出的重传，在网络丢失了初始注册请求的情况下，不需要家乡代理启动另一次“即时”机制重新和移动节点同步．

(2) 注册消息

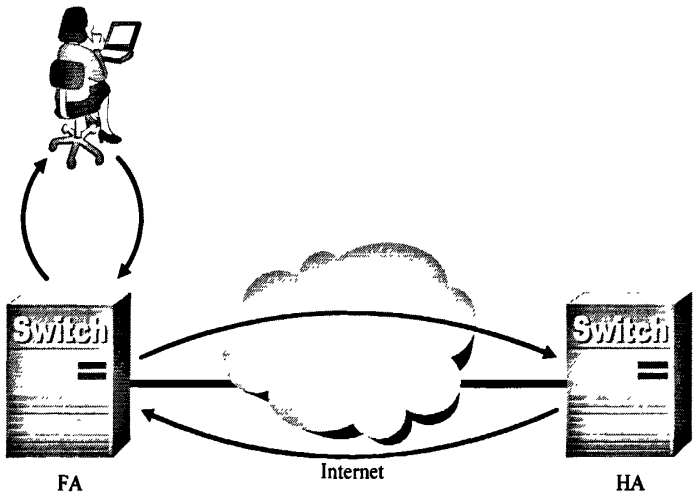

图 3.1 移动 IP 注册(用外地代理转交地址)

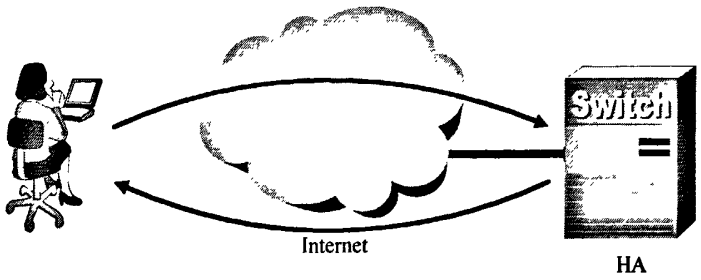

图 3.2 移动 IP 注册(用配置转交地址)

注册消息被封装在 UDP 报文的数据字段，使用端口为 434．注册消息由注册消息的移动 IP 字段加上可选的扩展字段、移动家乡认证扩展以及其他可选扩展部分构成[36]．在注册过程中交互发送的消息分为两种：注册请求消息和注册应答消息．注册请求消息的结构包括类型、设置字段、生存期、家乡地址、转交地址、标识和扩展等部分．注册应答消息包括类型、编码、生存期、家乡地址、标识和扩展等部分．

注册消息的发送被定义为两种不同的过程，当移动节点获得的转交地址是配置转交地址时，移动节点和它的家乡代理之间通过一次注册请求和注册应答交互来完成消息注册(图 3.1)．当转交地址为代理转交地址时，移动节点则是通过外地代理转发注册请求(图 3.2)．

这两种注册过程都包含了注册请求和注册应答消息的交换．如果移动节点直接到自己的家乡代理进行注册，注册过程只需要下面两个消息：

- 移动节点发送注册请求给家乡代理；
- 家乡代理给移动节点发送一个注册应答，同意或者拒绝这个请求．

如果注册需要通过外地代理，则注册包括以下四个消息：

- 移动节点发送注册请求到预期的外地代理，开始注册过程；
- 外地代理处理注册请求，然后把它转发到家乡代理；
- 家乡代理发送注册应答到外地代理，同意或者拒绝这个请求；
- 外地代理处理注册应答，把处理的结果告知移动节点．

3.2　移动 IP 注册协议的安全性

3.2.1　移动 IP 注册协议的安全要求

网络安全的目标包括机密性、完整性、安全认证、可靠性、可用性、授权访问、责任、担保和隐私保护等[34]．对于移动 IP 网络，由于其自身特点的原因，其所遭受的安全性风险更大．特别是在电子商务或者电子政务等的应用中，保密性和认证等要求显得尤为重要．针对移动 IP 网络的特点，我们将其安全性要求总结如下：

(1)　保密性

保密性就是保证机密信息和数据部会泄露给非授权的用户．除了要保证通信数据的机密性外，对于移动 IP，要特别关注以下信息的机密性．

- 用户信息

所有的通信系统都采用某种用户 ID 来标识用户，移动用户在使用服务或进行

电子商务交易时，通常也要提供诸如信用卡号、银行账号及对应的口令等敏感信息．所有这些信息都是网络黑客感兴趣的，因而必须采用强的加密方式，保证其秘密性；否则，这些机密信息一旦泄密，将会给用户造成不可估量的损失．

• 用户位置

移动环境中，用户使用的无线信号容易泄漏用户的位置信息，移动IP的一些信令中也会包含用户当前所在网络的信息，但是，有些用户并不希望系统中的其他用户获取该信息．用户应该有权选择自己的位置信息是公开还是保密，这样，既能在需要时获得相应的服务，又能保留一定的隐私．

• 呼叫模式

呼叫模式是指呼叫者ID、呼叫的频率、经常呼叫的通信对方等信息，窃听者一旦掌握了用户的呼叫模式，就更容易发起攻击．

(2) 认证

认证就是识别和证实，识别是辨别一个对象的真实身份，证实是证明该对象的身份就是其声明的身份．

在移动通信中，客户经常要使用外地网络的资源．通常这些资源不是免费向公众开放的，只有授权后的客户才能访问．授权访问的前提是认证．在商业的移动IP网络中，对所有外地代理和家乡代理之间的消息进行认证是重要的，这样才可能计费．而认证是多种多样的，既有被访问网络和家乡网络对移动节点的认证，也有被访问的网络对移动节点家乡网络的认证，还可能需要服务级的认证．所有这些认证必须是强认证的，而且提供不可抵赖功能．在认证的基础上，确定移动用户的权限，实现授权访问，同时根据用户使用的服务进行记账．关于认证、授权和记账的在移动IP中的应用已经超出了本论文的研究范围．

(3) 信息完整性

信息完整性就是保证信息和数据的一致性，防止信息和数据被非授权用户利用、修改和破坏．

(4) 服务可用性

移动IP的协议实体包括：移动节点、外地代理、家乡代理和通信对端．这些协议实体都可能遭受安全攻击，因此，应该从以下几个方面考虑移动IP的安全要求．

• 移动节点：当访问外地子网时，要能够获得网络服务并且保护通信过程．

• 外地代理和被访问子网：当移动节点访问时，要能够保护网络的资源和本地通信流．

• 家乡代理和家乡网络：移动节点离开家乡网络，要能穿越家乡网络的防火

墙；要防止恶意节点通过仿冒移动节点入侵家乡网络.

• 通信对端：要防止恶意节点假冒移动节点进行会话窃取的攻击.

为了满足以上移动 IP 安全性方面的要求，移动 IP 注册协议在设计的时候必须满足：实现移动节点，外地代理和家乡代理之间的相互认证、数据的完整性、消息的新鲜性、移动节点的用户匿名性、会话密钥的安全协商以及密钥更新.

3.2.2 移动 IP 注册协议安全威胁和攻击

当移动节点移动到外地网络，获得转交地址之后，必须进行移动注册. 移动节点向家乡代理发出注册请求，家乡代理返回注册应答，这样保证发往移动节点的分组能够正确路由到移动节点. 然而，由于移动 IP 网络中介质的开放性、无线网络自身的特点，移动 IP 的安全问题成为其能否得到大规模应用的关键因素.

目前，针对移动注册的攻击有以下几种.

(1) 拒绝服务攻击

拒绝服务攻击是指非法人员为了阻止他人正常接收服务而采取的一种攻击方法. 在已知的移动 IP 协议安全性威胁和攻击当中有相当一部分属于这种类型，同时它也是目前面临的最严重的一种攻击. 主要包括以下两种形式：一是非法人员向主机发送大量的数据包，使得主机的 CPU 忙于处理这些无用的信息，导致他人的请求无法得到正常响应；二是非法人员对网络上的两节点间传送的数据包进行干扰，使得数据传输不能正常进行.

对于第一种攻击中，最常见的攻击方法是 TCP 序列号轰炸攻击[15,37]. 非法人员使用大量非法的源地址建立 TCP 连接来“轰炸”目标主机. 这种攻击方法对于采用 TCP/IP 协议的网络都有效果，是利用 TCP/IP 协议自身的设计缺陷进行的. 它能够成功的一个关键原因在于目前 IP 单播数据包的选路只依赖于目的地址，而不需要查看源地址. 这种特性使得攻击者可以用假冒的 IP 地址不断地发送请求数据包，达到耗尽服务器资源的目的. 对于 TCP 序列号轰炸攻击目前没有彻底解决的办法，但是可以通过检查数据包的源地址、入口过滤等方法减轻其造成的危害.

对于第二种形式的拒绝服务攻击[38]，在移动 IP 网络中和在传统的互联网中不同的是，攻击并不要求攻击者位于两个通信节点之间的路径. 如果移动主机位于外地链路上，它必须向家乡代理注册它的转交地址，然后由家乡代理根据注册的转交地址通过隧道技术将数据包传送到移动主机. 所以一个攻击者只需要简单地发送一条伪造的注册请求给家乡代理，以它自己的 IP 地址代替移动节点的转交地址. 如果攻击者的注册成功，那么它就可以截获本应送往移动节点的数据包，从而使得移动节点得不到服务. 目前，这种攻击主要分为三种：攻击者将绑定更新消息中的转交地址设置为虚假地址，从而伪造的注册请求，中断移动节点的可寻

址性；攻击者将绑定更新消息中的转交地址设置为自己的 IP 地址，进行信息窃取；攻击者用其他受害者的 IP 地址代替转交地址，进行反射攻击.

另外，非法人员还可以通过假冒外地代理来对移动节点发起拒绝服务攻击[39]. 当移动节点收到代理广播消息时，它需要知道这条消息是否来自合法的外地代理. 如果没有认证机制，一个恶意的节点可以很容易冒充成一个合法的外地代理，然后以下面的方式进行拒绝服务攻击：

• 向移动节点返回注册应答消息告知其注册请求消息被拒绝了；

• 将移动节点的注册请求消息传递到另外的地址上，而不是传递到家乡代理上，使移动节点永远也接收不到来自家乡代理的注册应答消息；

• 将移动节点的注册请求消息丢弃掉，使其永远也接收不到来自家乡代理的注册应答消息.

对付拒绝服务攻击的解决方法是要求移动节点和它的家乡代理之间交互的所有注册信息都必须进行有效的认证，有效的认证使非法人员几乎不可能产生一个伪造的且不被家乡代理识破的注册请求消息.

(2) 重放攻击

重返攻击顾名思义即是将在不安全的无线信道上截获的消息重新发送的一种攻击方法. 针对移动 IP 注册协议的重放攻击主要包括以下两种：一是向家乡代理重发消息进行攻击；二是向外地代理重放注册消息进行攻击.

第一种重放攻击实际上是一种典型的假冒攻击[40]. 攻击者通过窃听会话，截取数据包，把一个有效的注册请求信息保存起来. 然后等待一段时间后，重放这个注册请求向家乡代理注册一个伪造的转交地址，使得家乡代理转发分组到这个以前的转交地址，从而达到攻击的目的. 攻击者发出一个伪造的注册请求，把自己的 IP 地址当作移动节点的转交地址时，通信节点发出的所有数据包都会被送给攻击者. 此时，攻击者能看到每一个送给移动节点的数据包；然而，移动节点无法再接收任何数据包，造成通信的中断. 进行这样的攻击对攻击者来说轻而易举，攻击者可以从无线网络覆盖的任何角落进行这种假冒攻击，它只需向移动节点的家乡代理发送一条伪造的注册请求消息. 这种攻击也可以看作是第二种形式的拒绝服务攻击.

第二种重放攻击是为了免费使用外地网络的资源[41-42]从而向外地代理发送截获的消息进行欺骗. 攻击者通过窃听，把一个以前有效的注册请求消息及其相应的注册应答消息保存起来，然后截获发往外地代理的注册请求和注册应答消息，依次重放这个保存的注册请求和注册应答消息，使得外地代理相信这是由合法的移动节点和家乡代理发送的，从而欺骗了外地代理，达到免费使用外地网络资源的目的.

为防止重放攻击的发生，移动节点为每一个连续的注册消息标识域产生一个唯一值．利用这个值，家乡代理可以知道下一个值应该是多少，从而使得被非法人员保存下来的注册消息被家乡代理判定为已经过时的注册消息而不予处理．针对重放攻击，移动 IP 定义了两种填写标识域的方法．一种方法利用时间戳，另一种方法是采用随机数算法．

(3)　中间人攻击

中间人攻击是指非法人员利用技术手段将自己控制的主机充当中继主机从而达到攻击目的的一种攻击方法．攻击者假冒外地代理，并广播自己的代理广播消息．然后中继移动节点的注册请求和家乡代理的注册应答消息，这样移动节点和家乡代理之间通过该攻击者执行移动 IP 通信．攻击者的目的是窃听通过它的通信信息．

经典的密码协商方案 Diffie-Hellman 密钥协商方案不能抵御这种攻击．攻击者 Eve 截取密钥协商双方之间交换的信息并替换成自己的信息．从而攻击者就与协商密钥的双方(假设为 Alice 和 Bob)分别“建立”了秘密密钥，当 Alice 要加密一条消息发送给 Bob 时，Eve 可以解密而 Bob 却不可以(对于 Bob 向 Alice 发送消息的情况类似)．有一个更有效的方法可以用来设计密钥协商方案，即在密钥建立的同时就要认证参与者的身份．这种类型的密钥协商方案被称为认证密钥协商方案．本文提出的 MN 和 HA 密钥协商的方案即亦起到了认证的效果．

(4)　被动窃听

被动窃听是非法人员通过传输介质上直接窃听传输信息的攻击方法．

在移动 IP 网络中，我们需要保证以下两种信息的保密性：一种是在移动实体之间交换的秘密信息，比如密钥；另一种是移动用户的身份信息．通过秘密窃听通过移动用户的数据分组流，攻击者能够得知移动用户的真实身份，跟踪移动用户的移动轨迹和当前的位置而不被它发现，这严重侵犯了个人隐私．在移动通信时代即将来临的今天，越来越多的业务需要通过移动通信来完成．语音服务不再是移动通信的主要业务，取而代之的是数据业务，包括手机下载、在线视频，收看电视节目等．同时在移动通信中，办理银行、公司业务将是人们的生活变得更加方便．此时，移动通信用户的匿名性、密码口令等的保密性将更加重要．

(5)　恶意攻击

恶意攻击是指非法人员在任何位置接入移动 IP 网络，随意地篡改、截获两个节点之间的通信信息，对网络造成破坏的一种攻击．由于 Internet 和无线环境的开放性，这种攻击具有一定的破坏性．同时，节点无从得知它们的通信被破坏．这个攻击的目的就是破坏网络中的通信，他并不关心移动 IP 注册协议的细节．

要防止这种攻击，首先得保证非法人员无法与网络上的其他节点通信，因此必须保护好网络的物理安全．在会话可能被窃取的物理链路上不应该有任何节点，移动节点和固定节点都应该从这样的链路上移走．同时对所有合法的节点至少使用链路层以上的加密.本文在移动IP安全性方面的研究主要针对移动IP协议本身，我们希望通过设计更加良好性能的协议来提高安全性．故对恶意攻击的攻防不在本论文的研究范围之内．

3.3 基于身份的移动IP注册协议

随着对发展移动互联网的迫切需求，移动IP技术越来越受到人们的关注．而如何对安全性及效率方面的诸多问题中达到平衡，则成为移动IP技术能否在各种新型网络中广泛应用的关键．其中包括，注册节点认证的安全性、用户位置的保密性、降低有限资源终端计算量等问题．

针对无线网络认证的相关问题，文献[43]提出了一种对称加密方案，大大提高了协议的效率，但是同时也存在着严重的安全问题．文献[44]针对文献[43]的协议做了改进，并给出了形式化的证明，但改进后的协议比较复杂．文献[45]利用基于身份的理论提出了一种新的方案，不过该协议的移动节点在计算会话密钥时多次涉及双线性对运算，计算量大．文献[46]针对以上各种协议中存在的问题，利用Diffe-Hellman 密钥交换机制来构造注册请求消息中的临时身份标识符，极大提高了效率．

本章提出的移动IP注册协议[47]，其安全性基于椭圆曲线中双线性对的困难问题，并据此提出一种新的密钥协商与发放方案．该方案不仅能实现认证安全以及用户保密性、减小移动节点的计算量，而且具有密钥更新方便、计算负担小等优点．

本协议中用的符号说明如下：

ID_{MN}：移动节点MN的身份标识；

ID_{HA}：家乡代理HA的身份标识；

ID_{FA}：外地代理FA的身份标识；

HoA_{MN}：移动节点的家乡地址；

CoA_{MN}：移动节点的转交地址；

k_{MN-HA}：移动节点MN与家乡代理HA的共享密钥；

k_{MN-FA}：移动节点MN与外地代理FA的共享密钥；

$\langle M \rangle_k$：消息 M 在密钥 k 下的消息认证码（MAC）值；

$Sig(k_{HA-S}, M)$：使用私钥 k_{HA-S} 对消息 M 进行的数字签名.

3.3.1 系统建立

(S1) 可信中心 TC，基于安全参数生成阶为素数 q 的加法群 G_1 和乘法群 G_2. 其中，$P(P \in G_1^*)$ 是 G_1 的生成元，$\hat{e}$ 是 $G_1 \times G_1 \to G_2$ 的一个双线性映射. TC 随机选择整数 $s(s \in Z_q^*)$，计算 $P_{TC} = sP$. s 是系统私钥，P_{TC} 是系统公钥. TC 选择杂凑函数 $H: \{0,1\}^* \to G_1$. 系统建立后公开系统参数<G_1，G_2，P，$\hat{e}$，P_{TC}，H>.

可信中心 TC 为家乡节点 HA 分配公钥 $Q_{HA} = H(ID_{HA})$，私钥 $S_{HA} = sQ_{HA}$.

(S2)有线网络中的可信中心 CA 分别给 HA 和 FA 颁发证书 $Cert_{HA}$、$Cert_{FA}$，其对应私钥分别是 k_{HA-S}，k_{FA-S}.

3.3.2 用户登记

当用户 MN 要注册为 HA 的用户时，首先 HA 为 MN 分配一个唯一的用户标识符 ID_{MN}，接着由 TC 为 MN 分配一密钥对，其中公钥 $Q_{MN} = H(ID_{MN})$，私钥 $S_{MN} = sQ_{MN}$. 其次，HA 秘密地保存着一个随机数 $h(h \in Z_q^*)$，并保存记录<Q_{MN}，h，ID_{MN}>. 最后，HA 计算 $k_1 = \hat{e}(Q_{HA}, P_{TC})$，$k_2 = \hat{e}(Q_{MN}, t_{HA})$(其中 $t_{HA} = hP$)，将 k_1，k_2，ID_{MN} 存储于智能卡里通过安全信道交给 MN.

3.3.3 认证过程

协议的描述如图 3.3 所示.

• 代理广播：

FA→MN:

Advertisement，ID_{FA}，CoA_{MN}，$Cert_{FA}$.

外地代理发布通告消息，其中包括外地代理的 ID 号、代理转交地址和外地代理的证书等.

• 注册：

(R1) MN→FA：M_1，$\langle M_1 \rangle_{k_{MN-HA}}$.

M_1 包括 Request，ID_{HA}，CoA_{MN}，T_{MN}，ID_{FA}，Q_{MN}，t_{MN}.

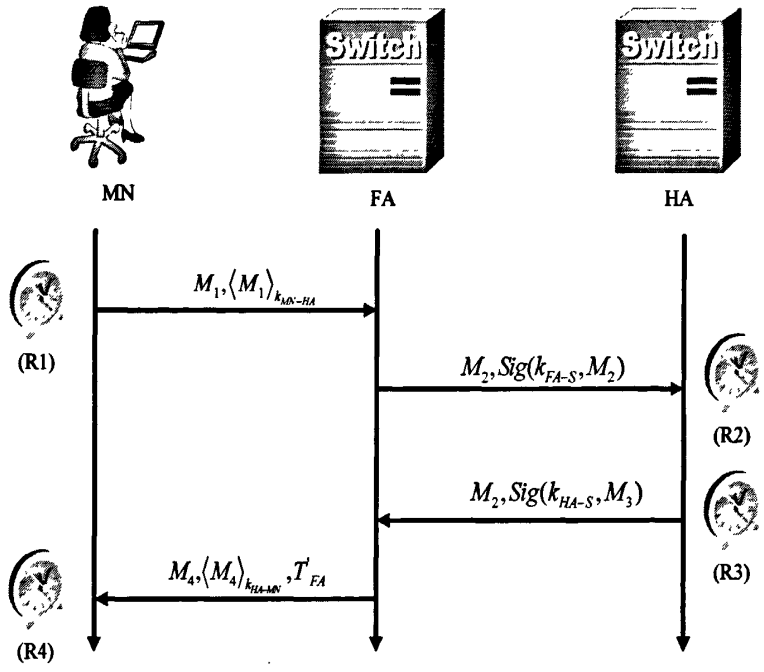

图 3.3 基于 ID 的移动 IP 注册协议

MN 选择一个随机数 $m\left(m\in Z_q^*\right)$，计算 $k_{MN-HA}=k_1^m\cdot k_2$，$t_{MN}=mP$，获取当前时戳 T_{MN}．然后求出消息在密钥 k_{MN-HA} 下的消息认证码作为 MN 和 HA 之间的认证扩展．

(R2) FA→HA：M_2，$Sig\left(k_{FA-S},M_2\right)$．

M_2 包括 M_1，$\langle M_1\rangle_{k_{MN-HA}}$，$ID_{FA}$，$Cert_{FA}$，$T_{FA}$，$t_{FA}$．

FA 检查 T_{MN} 是否新鲜，为 MN 选取一随机数 $f\left(f\in Z_q^*\right)$，计算 $t_{FA}=fP$．然后，FA 获取当前时戳 T_{MN}，连同转发信息、自己的公开信息签名后发送给 MN．最后，FA 在空余时间计算共享密钥 $k_{FA-MN}=ft_{MN}$．

(R3) HA→FA：M_3，$Sig\left(k_{HA-S},M_3\right)$．

M_3 包括 M_4，$\langle M_4\rangle_{k_{HA-MN}}$，$Cert_{HA}$，$T_{HA}$；$M_4$ 包括 Reply，Result，HoA_{MN}，ID_{HA}，k_2'，t_{FA}．

HA 首先检查 T_{FA} 是否新鲜，在 M_1 消息块里的 ID_{FA} 与消息块之外附加的 FA 公开信息中的 ID_{FA} 是否一致，然后验证 FA 的签名．如果验证成功，则 HA 通过对 FA 的认证．

HA 在消息 M_2 中找出申请注册节点的公钥 Q_{MN} 和 t_{MN}，在记录中查找相应的随

机数 h，计算 $k_{HA-MN}=\hat{e}(hQ_{MN},P)\cdot\hat{e}(S_{HA},t_{MN})$，验证 $\langle M_1\rangle_{k_{MN-HA}}$ 成功则 HA 通过对 MN 的验证.

HA 为 MN 动态分配一个家乡地址，并把家乡地址与接收到的转交地址绑定起来.然后为 MN 重新选定一个随机数 $h'\left(h'\in Z_q^*,且h'\neq h\right)$，并重新计算 $k_2'=\hat{e}(Q_{MN},t_{HA}')$ (其中 $t_{HA}'=h'P$). 在获取当前时戳 T_{HA} 之后，HA 对要向 MN 回复的消息计算密钥 k_{HA-MN} 下的 MAC 值. 然后用自己的私钥 k_{HA-S} 对 M_3 进行数字签名并将消息和签名发送给 FA.

最后，HA 在注册空余时间，计算新的会话密钥 $k_{HA-MN}'=\hat{e}(h'Q_{MN},P)\cdot\hat{e}(S_{HA},t_{MN})$，并更新记录.

(R4)　FA→MN：M_4，$\langle M_4\rangle_{k_{HA-MN}}$，$T_{FA}'$.

FA 检查 T_{HA} 是否新鲜，然后验证 HA 的签名是否正确，若正确则 FA 完成对 HA 的验证.

MN 从 FA 收到信息后检查 T_{FA}' 新鲜，然后验证 M_4 的消息认证码，若正确则 MN 完成对 HA 进行认证. 同时 MN 在获得 t_{FA} 之后，计算 MN 与 FA 的共享密钥 $k_{MN-FA}=mt_{FA}$，在获得 k_2' 之后，计算 MN 与 HA 之间的共享密钥 $k_{MN-HA}'=k_1^m\cdot k_2'$，用作下一次注册请求消息的认证. 更新共享密钥可在移动节点的空余时间进行，并不影响节点的切换效率.

3.4　安全性和效率分析

下面我们对于新协议进行的安全性分析. 对于效率分析我们主要采用的是分析注册消息大小、信息交互次数和移动节点计算量的方法. 因为移动节点往往具有有限的内存和计算能力，是影响整个切换效率的瓶颈. 减小移动节点的计算量即能显著提高注册协议的效率.

3.4.1　安全性分析

(1)　协议对于拒绝服务攻击是安全的

针对移动 IP 协议所采用的拒绝服务攻击大致分为以下两种：攻击者产生虚假注册信息进行攻击、攻击者截获注册回复信息使注册不能成功.

• 攻击模型一

攻击者用自己的 IP 地址来冒充注册者的转交地址，从而用伪造的注册请求信息来进行注册．一旦攻击成功，非法攻击者将能够得到通信对端发送的数据．

分析：攻击者用自己的 IP 地址来冒充注册者的转交地址，从而产生注册请求信息中的 $M_1^{'}$，但是攻击者却不能生成 $M_1^{'}$ 在密钥 k_{MN-HA} 下的消息验证码 $\langle M_1^{'} \rangle_{k_{MN-HA}}$．HA 在收到注册请求消息之后，根据注册节点的 Q_{MN} 在自己维护的用户信息表中查找其对应的 h 值，从而生成 k_{HA-MN}．在生成 k_{HA-MN} 之后，HA 验证消息 $M_1^{'}$ 在密钥 k_{HA-MN} 下的消息认证码．如果验证成功则 HA 通过对 MN 的认证，否则将会拒绝此注册请求．因此，本协议能够抵御此类攻击．

下面我们讨论一下，本协议是如何做到只有合法的移动用户自己能够生成用于生成消息认证的密钥[48]．

首先，由本文第二章中介绍的双线性对的性质可得，k_{MN-HA} 和 k_{HA-MN} 是相同的．推导如下：

$$
\begin{aligned}
k_{MN-HAk} &= k_1^m \cdot k_2 \\
&= \hat{e}(Q_{HA}, P_{TC})^m \hat{e}(Q_{MN}, t_{HA}) \\
&= \hat{e}(Q_{HA}, P)^{ms} \hat{e}(Q_{MN}, P)^h \\
&= \hat{e}(sQ_{HA}, mP)\hat{e}(hQ_{MN}, P) \\
&= \hat{e}(hQ_{MN}, P)\hat{e}(S_{HA}, t_{MN}) \\
&= k_{HA-MN}
\end{aligned}
$$

其次，用户 MN 用于生成 k_{MN-HA} 的 k_1、k_2 值是在用户登记时通过安全信道获得的，而秘密随机数 m 是在注册时临时生成的．攻击者无法获知 k_1、k_2 和 m 来生成 k_{MN-HA}．同时，攻击者在不知道保存于 HA 处 MN 对应的随机数 h 和 HA 私钥的情况下，亦不能生成 k_{HA-MN}．

此外，攻击者还可能将注册者的转交地址伪造为无效地址使注册不能成功，或者转交地址伪造为其他受害者的地址．不过此伪造的注册请求消息同样不能在 HA 处注册成功．

• 攻击模型二

攻击者截获由 FA 返回 MN 的注册回复信息，使得 MN 不能注册成功．

分析：当注册节点遭到此类攻击，即在注册请求发出后预定时间内未能收到

注册回复消息的情况下，之前代理处的密钥跟新信息将作废．具体做法是，注册节点在预定的请求次数内仍然没有收到注册回复消息，将采用初始的k_2来生成注册请求信息重新注册．家乡代理在对发出注册请求消息验证不成功的情况下，将采用初始h重新计算$k_{HA\text{-}MN}$，若能够通过将重新发送跟新后的k_2值．

(2)　协议对于重放攻击是安全的

针对移动 IP 协议的重放攻击也包括两种：攻击者向 HA 重新发送注册请求消息、攻击者向 FA 重新发送注册请求或者回复消息．

• 攻击模型一

攻击者截获并保存一个先前已经被 HA 成功接收的注册请求消息．等到移动节点离开该外地代理后，攻击者向 HA 重新发送该请求消息，以便把发送给 MN 的数据包仍然定向到以前所处的位置．

分析：FA 向 HA 发送的注册请求中包括发送消息时的时戳T_{FA}，而该消息还附带有 FA 的数字签名，故攻击者不能更改请求消息中的时戳．HA 在收到请求消息后，需要查看消息中附带的时戳，已确保消息的新鲜性．所以，本协议可以抵御此类攻击．

• 攻击模型二

攻击者向 FA 重放由注册节点发来的注册请求信息或者由 HA 发来的注册回复信息．

分析：移动节点 MN 向 FA 发送的注册请求中包括发送消息时的时戳T_{MN}，并且该消息附带有消息验证码．即使攻击者更改了请求消息中的时戳，但是无法伪造消息验证码．所以由 FA 转发的伪造之后的请求消息依然会被 HA 拒绝．从这里我们可以看出，本协议 FA 和 MN 的相互认证是通过 FA 和 HA、HA 和 MN 的相互认证实现的．其中，FA 和 HA 的相互认证时通过各自的公钥证书和数字签名实现的．消息接收方可以根据发送方公钥证书中提供的签名公钥验证对方的数字签名，以证实对方的身份．

HA 向 FA 发送的回复消息中包括发送消息时的时戳T_{HA}，而消息中附带的签名能够保证时戳不被修改，从而保证了消息的新鲜性．

综上所述，本协议可以抵御重放攻击．

(3)　协议对于中间人攻击是安全的

中间人攻击是指，攻击者假冒中间人 FA 来窃取 MN 和 HA 之间的注册信息.

分析：FA 在收到注册节点的注册请求消息之后，增加外地家乡代理之间的认证扩展，并且对发往 HA 的消息进行签名. FA 增加的认证扩展中包括 FA 的证书 $Cert_{FA}$，HA 可以在获取 FA 的证书之后来验证 FA 的签名，以实现对 FA 的认证. 所以，协议对于中间人攻击是安全的.

(4) 协议对于被动攻击是安全的

被动攻击分为以前两种：窃听链路上传输的密钥等秘密信息、窃听 MN 的身份信息.

• 攻击模型一

分析：本协议中的密钥协商方案，生成密钥均在本地进行.

MN 和 HA 共享密钥：MN 端通过在用户登记时获得的 k_1、k_2 和自己生成的随机数 m 计算所得，而 HA 端则通过对应了 MN 的随机数 h、由 MN 发送来的 t_{MN} 和自己的私钥计算所得. 在链路上监听所得到的任何信息都不能生成共享密钥.

MN 和 HA 密钥更新：当 MN 注册完成需要更新密钥时，HA 由自己更新过的随机数 h' 计算出 k_2' 发送给 MN. 而 MN 只需要跟新 k_2 为 k_2' 便可以计算出新的会话密钥 $k_{MN-HA}' = k_1^{m'} \cdot k_2'$.

MN 与 FA 的密钥更新：MN 与的 FA 的会话密钥采用基于身份的 Diffe-Hellman 密钥交换机制. 双方只需发送新的随机变量 t_{MN}、t_{FA} 即可实现密钥更新.

故本协议可以抵御此类攻击.

• 攻击模型二

分析：本协议可以实现用户的匿名性. 在协议的传输过程中，用户的真实 ID 并没有在发送的请求消息之中. MN 发送的请求消息中只包含自己的公钥 Q_{MN}，HA 可以通过 Q_{MN} 在用户登记表 $\{Q_{MN}, h, ID_{MN}\}$ 中能够查询到用户的真实身份信息，其他人均不能获得任何关于用户的身份信息.

3.4.2 效率分析

对于移动 IP 注册协议的效率我们主要从时延的角度来分析. 设计一个好的注册协议即要在保证安全性的前提下，注册信息交互少、注册消息小以及节点进行密码算法处理时操作时间短. 这样即能缩短注册时的时延. 本节选取了与本协议

同样具有较高安全性保证的文献[44]、文献[46]进行效率分析.

本文设计的协议，通过移动节点与外地代理、外地代理和家乡代理的一次信息交互即实现了认证三方的两两认证. 移动节点与外地代理之间，采用椭圆曲线下的 Diffie-Hellman 密钥交换算法. 移动节点与家乡代理之间则利用双线性对的性质，设计了一种巧妙的认证方案. 这样无需系统为移动节点每次的移动分配密钥，同时也增强了协议的安全性. 在移动用户的信息交互次数方面，文献[44]和文献[46]也和本协议一样均进行了一次交互.

在协议的消息中，包括家乡代理的地址，转交地址，时间戳等. 而真正会使得注册消息过大以致增加时延的只能是扩展部分. 本文设计的协议，在移动节点发往外地代理的消息中，扩展部分仅包括移动节点的随机变量以及消息认证码. 消息认证码不仅能保证注册消息的完整性，而且能够使 HA 对 MN 的身份加以认证. 因为家乡代理可以用随机变量生成计算消息认证码的密钥，而此密钥只有消息发送方和 HA 才能生成. 文献[44]和文献[46]则除了随机参数外，在注册请求消息中还包括了加密的临时身份标识符，而本章所提出的方案中，用于生成消息认证码的密码则兼有临时身份标识的作用.

在考虑了信息交互次数和注册消息大小这两个因素之后，我们再来看移动节点的消息处理时延. 移动节点因为内存小、计算能力不足等原因容易造成无线通讯的延时，从而影响整个协议的效率. 也就是说移动节点的处理时延是整个注册时延的瓶颈，只要我们将移动节点的计算时延降低，注册时延也将随之降低.

下面是本协议在减小移动节点 MN 计算量问题上的解决思路. 在移动 IP 协议中，安全和效率始终是一对相互制约的因素. 在不出现新的密码算法的前提下，比较小的计算量必然会导致安全性的下降. 所以，我们在设计本章所提出的协议时，我们的思想是尽可能将计算量“转移”到代理中. 由代理计算移动节点认证时所计算的中间量，然后发送给移动节点. 这样可以使协议在保证安全性的前提下提高效率.

对于以下几种满足安全性的无线认证协议我们对移动节点 MN 做了如下的效率分析：

在比较各个协议中移动节点的计算量之前，我们将各种密码运算的计算处理时间列表如表 3.1 所示，其中数据由文献[49]所得. 下面中计算各密码算法的处理平台是 Pentium 4 2.1 GHz 处理器，运行 Windows XP SP 1.386. 由表 3.1 可知，在相同的数据长度下，计算双线性对所需的处理时间最长，其次是指数运算和椭圆曲线下的点乘运算. 对称加密和哈希运算的处理时间通常比以上三者要小 103 倍，且对称加密的处理时间少于哈希运算. 异或运算所需处理时间极小，相对于其他运算可忽略，故下表未列出.

表 3.1 数据长度为 2k bits 时 MN 端操作的运算时间

Processing time	
Exponentiation	4.75ms
SHA	0.000898ms
Scalar Multiplication	0.43ms
DES	0.000358ms
Pairing Operation	4.3ms

表 3.2 几种安全协议中移动节点计算量分析

	指数运算	哈希运算	点乘	对称加/解密	异或运算
文献[36]	2	2	0	3	2
文献[38]	2	3	0	0	1
本协议	1	2	1	0	0

本协议与文献[44]和文献[46]相比，均少了一次指数运算，多了一次点乘运算. 此外，文献[44]还需要再多 3 此对称加/解密运算和 2 次异或运算，文献[46]比本协议还要再多进行一次 hash 运算，一次异或运算. 在同样的消息长度前提下，点乘运算的处理时间比指数运算要小. 综上所述，本协议在移动节点端的计算量明显减少. 另外，本协议最主要的特点是在密钥更新时计算量小，易于减小 MN 频繁微移动而引起的密钥更新计算，具有一定的实用价值. 而在文献[46]中并未明确分析密钥更新所需的计算代价. 文献[46]在计算与家乡代理和外地代理的共享密钥时，分别需要进行 1 次指数运算，1 次 hash 运算，而本文的协议只需要做 1 次点乘和 1 次乘法.

综上可知，本文所提出的协议不仅有很好的安全性，效率也有了较大的提高，并且更具有实用价值.

3.5 本章小结

本章首先对移动注册协议及其注册消息做了阐述，然后介绍了移动 IP 注册协议的安全性要求和常见的安全威胁. 采用一种新的密钥协商方案，设计出一种基于身份的移动 IP 注册协议，并且给出了其安全性和效率分析. 注册协议是移动 IP 切换中的重要部分，注册协议和其中认证算法的设计对移动 IP 切换机制的安全和效率有着非常重要的影响.

第四章　基于身份的层次化移动 IPv6 切换技术

移动 IP 的切换技术是移动 IP 应用的瓶颈. 目前，研究针对不同的目的和应用场景提出了各种切换技术. 本章首先对各种切换技术作了概述，对文献[25]中的 2 层认证协议进行了改进，接着提出了一种层次化移动 IP 与组播技术相结合的方案. 最后的安全性和效率分析指出，该方案在保证安全性的前提下因为切换产生的延时问题也有了明显的改善.

4.1　移动 IPv6 切换技术

4.1.1　移动 IPv6 切换技术分类

(1)　基于微移动的切换技术

其基本思想是引入一个新实体本地家乡代理来管理本地的运动. 这样当 MN 在一个局部管理域移动时，只需向本地家乡代理登记；只有在局部管理域之间运动时，才会向 HA，CN 执行位置登记.

(2)　基于位置的切换技术

在移动环境下与静止环境下进行通信，一个巨大的区别就是 MN 需要不断地判断自己的物理位置是否发生了变化. 在基本移动 IP 中，主要采用时间检测和前缀匹配检测来推断是否发生移动. 然而，MN 的运动实质上就是物理位置的改变. 因此，一个非常自然的思路是可以直接利用 GPS 信息，去计算物理位置的变化.

(3)　基于组播的切换技术

组播技术提供了支持 IP 移动的另一种途径. 目前，有三类组播技术来增强基本移动 IP 的性能：PIM/DM、PIM/SM、SGM.

(4)　基于暗示的切换技术

在移动 IP 中，协议层之间的分离，是增大时延的根源. 因此，打破协议层之间的独立性是减少时延的根本途径. 这种方法，利用链路层的信息，来“暗示”IP 层将要发生切换. 因此又称为基于暗示的切换策略.

(5)　基于链路层的切换技术

为提高移动 IP 的性能，上述提出的各种快速切换技术，都对移动 IP 作了或多

或少的修改. 另一种思路是在不改变移动 IP 协议的前提下，通过增强或改变链路层技术来达到快速切换的目的.

4.1.2 几种重要的移动 IPv6 切换技术

(1) 移动 IPv6 快速切换技术

快速切换是一种通过提前注册，以及在新的外地网络切换未完成时通过与前一个网络保持通信实现快速切换，并且能为一堆实时业务提供切换支持的操作技术.

移动 IPv6 快速切换技术是对移动 IPv6 协议的改进，可以加快 IPv6 移动节点的切换过程，减少已有通信连接的中断时间，保证通信流的实时传输. 它的主要功能是能够减小或者消除了移动节点建立新的通信路径的延迟.

接入路由器(AR)是指网络和移动主机之间的最后一个路由器. 通过在接入路由器之间以及接入路由器、移动主机之间加入一些新消息，可以实现快速的切换. 快速切换可以很容易地在移动主机移动到新接入路由器之前，为其配置转交地址. 当移动主机连接到新接入路由器时，就可以立刻使用该转交地址. 在此之前，需要进行的准备工作包括新转交地址配置、重复地址检测和邻居发现等. 当不能从新接入路由器获得有效的转交地址时，快速切换也允许移动主机不获得新转交地址而切换到新的网络.

移动 IPv6 快速切换技术采用预先切换和基于隧道的切换两种机制. 预先切换是指当移动节点和旧接入路由器还保持着 2 层连接时，就发起第 3 层的切换. 基于隧道的切换是指当移动节点与新接入路由器的第 2 层连接已经建立时，还不启动第 3 层的切换以获得新的转交地址，而是在两个网络的 AR 之间建立隧道传输分组，尽量较少实时流的中断时间.

(2) 移动 IPv6 平滑切换技术

移动 IPv6 平滑切换技术是一种使用移动 IPv6 中的“绑定更新”消息携带转移状态信息，使得切换能够具有低延迟、低分组丢失和移动节点通信中断减小的切换技术.

随着 VoIP 等实时应用程序的出现，移动 IP 中的切换效率变得非常重要. 当运行实时应用程序的移动节点进行切换时，需要切换尽量平滑. 对于实时传输，在切换的过程中不仅要使切换速度快，还要考虑状态信息的转移等问题.

对于平滑切换，给出了对移动 IPv6 的扩展，在切换时通过附加控制结构传输必要的状态信息，这样在切换时，运行在移动节点上的应用程序能保持较低的延迟、最小的中断和减小的数据包丢失率. 而且，当移动节点在同一个访问域内移动时，移动 IPv6 区域注册减小了绑定更新信令延迟和信令负载. 延迟的减小是通

过将绑定更新限制在本地，而信令负载的减小是因为采用了区域感知路由器地址作为代理转交地址或者区域转交地址．区域注册可以采用区域感知路由器的任意播地址，在相关路由器上为移动节点生成宿主路由器，支持任意的层次拓扑结构，不需要知道从其他域移动过来的移动节点的其他信息，并且制定了转交数据包的最佳方法，与平滑/快速切换相兼容．

要在移动网络中支持实时应用程序如 VoIP，需要考虑的一个重要问题就是平滑切换的能力．当移动节点在网络链路中移动时，平滑切换能最小化数据包丢失率．定义了移动 IP 的一种缓存机制，移动节点要求当前子网的路由器缓存它的数据包，直到移动节点完成向新子网内路由器的注册过程．一旦注册完成，移动节点在新网络中就有了合法的转交地址，缓存的数据包从先前的路由器转发过来，这样就减小了移动过程中的数据包丢失的可能性．

(3)　层次化移动 IPv6

层次化移动 IPv6(HMIPv6)是一种通过使用本地层次型结构，减少与外部网络的信令交互，减少切换引起通信中断时间的切换技术．

在 HMIPv6 中，引入一个新的实体，称为移动锚点(MAP)，它可以是层次型 IPv6 网络中的任何层次的路由器区，不需要每个子网都具有移动锚点．一个区域包含多个子网，子网的个数根据情况可以变化．每个子网都有接入路由器，每个区域有一个移动锚点．移动节点通过移动锚点获得的地址是指区域转交地址，可以使用区域转交地址向家乡代理和通信对端进行绑定，减少了在区域内子网间切换引起的通信中断时间．移动锚点的使用可以限制移动 IPv6 同本地域以外的节点的信令交互，它能支持快速移动 IP 切换，帮助移动节点实现无缝移动，并且支持特定的移动网络情况．关于层次化移动 IPv6 具体的切换模式和操作，我们将在下一节做详细的介绍．

4.2　层次化移动 IPv6 切换技术

4.2.1　协议概述

在移动 IPv6 协议的基础上，层次化移动 IPv6 协议中对移动主机和家乡代理的操作进行了少量扩展，没有对通信对端的操作进行修改．发生切换时，移动主机不是与原地的家乡代理，而是与本地 MAP 进行绑定更新，减少了切换的延迟．和移动 IPv6 相同，这一解决方案独立于下层接入技术，允许在不同类型的接入网络之间进行快速切换．

随着移动主机从一个子网移动到另一个子网，MAP 发现过程是连续进行的．当

移动主机在 MAP 域内进行漫游时，将收到同样的 MAP 通告信息．如果接受到的通告中 MAP 地址改变了，移动主机必须对这一改变进行处理，向家乡代理和通信对端发送必要的绑定更新消息．

如果移动主机在局部 MAP 域内改变了它的当前地址(链路转交地址 LCoA)，它只需要向 MAP 注册新的地址．因此，不需要改变通信对端和家乡代理上注册的 RCoA．移动主机与通信对端可以保持移动透明性．当移动主机使用 RCoA 地址时，MAP 就相当于移动主机的本地家乡代理，MAP 收到数据分组后使用隧道发送到移动主机的链路转交地址 LCoA．MAP 概念的引入使得移动主机在 MAP 域中改变它的三层访问点时，只需要向 MAP 执行一次本地的绑定更新．

层次型路由器可以是多级的，可以根据需要在接入路由器上实现 MAP 的功能．这样，移动主机可以选择第一跳 MAP 或第二跳 MAP．

移动主机通过 MAP 获得的地址是区域转交地址(RCoA)．根据移动记住 RCoA 用法的不同，有两种 MAP 模式：基本模式和扩展模式．当漫游到 MAP 域时，移动主机可以使用 RCoA 作为备用的转交地址(扩展模式)，或者在 MAP 的子网上形成自己的 RCoA(基本模式)．

4.2.2 基本模式

层次化移动 IPv6 的基本模式可以支持节点的移动．

在基本模式中，每个移动主机有两个转交地址：区域转交地址和链路转交地址．MAP 将移动主机的 RCoA 和 LCoA 进行绑定，而对于移动主机来说就相当于一个本地的家乡代理．

• 绑定更新

在移动到新的 MAP 域时，移动主机收到路由通告，从其 MAP 选项中获得 MAP 的网络前缀，使用无状态的方式形成 RCoA 和 LCoA．然后，移动主机向 MAP 发送一个绑定更新消息．绑定更新消息指定 RCoA 为家乡地址域，指定 LCoA 为源地址，不使用备用转交地址子选项．接着，MAP 将对移动主机的 RCoA 进行重复地检测．如果成功，绑定更新消息将移动主机的 RCoA 与 LCoA 进行绑定，MAP 将返回绑定确认消息到移动主机，指示注册成功；否则，MAP 必须返回带有相应故障代码的绑定确定消息．

移动主机收到从 MAP 发来的绑定确认消息后，需要将 RCoA 和家乡地址绑定．移动主机通过发送绑定更新消息到家乡代理，将新的 RCoA 注册到它的家乡代理，绑定更新消息的家乡地址域设为移动主机的家乡地址，转交地址子选项设为 RCoA．移动主机也可以向它的通信对端发送类似的绑定更新消息的源地址．向家乡代理和通信对端发送绑定更新消息时，移动主机也可以使用它的 RCoA 作为源地址．

• 数据转发

在基本模式下，MAP 的行为就像一个本地家乡代理，它截取所有发往移动主机的包，通过隧道发到相应的 LCoA. 为了加快 MAP 之间的切换速度，移动主机可以向它的前一个 MAP 发送绑定更新消息，制定它的新 LCoA，这样到达旧 MAP 的包可以被转发到移动主机的新 LCoA.

• MAP 域内切换

当移动主机进行本地移动时，它只需要向 MAP 注册新的 LCoA. 这种情况下，RCoA 没有改变，因此，也就不需要同家乡代理和通信对端重新绑定.

4.2.3 扩展模式

层次型移动 IPv6 的扩展模式可以同时支持节点移动和网络移动.

(1) 扩展模式对节点移动的支持

在扩展模式中，移动主机的 RCoA 是从邻居发现消息的 MAP 选项中得到的，这个 RCoA 被指定到 MAP 的某个接口上. 与基本模式不同，扩展模式中移动主机发出的数据分组不能使用 RCoA 作为源地址.

• 绑定更新

移动主机发现 MAP 后，可以向一个或多个 MAP 进行绑定. 移动主机向 MAP 发送的绑定更新消息中包含移动主机的家乡地址，并且使用 LCoA 作为转交地址. 当接受到移动主机发来的绑定更新消息后，MAP 必须首先检查是否移动主机被授权使用 MAP 的扩展模式. 如果检查通过，MAP 应该正常处理绑定更新包并将处理成功后的信息添加到绑定缓存中.

移动主机使用 RCoA 对它的家乡代理和通信对端进行绑定更新. 移动主机收到 MAP 对绑定更新消息的应答后，向家乡代理 HA 发送绑定更新. 在向家乡代理发送的绑定更新消息中使用 LCoA 作为源地址，在消息中还要包含移动主机的家乡地址，并且使用 RCoA 作为备用转交地址.

• 数据转发

MAP 将接受所有以移动主机为目的的分组，并且通过隧道发到移动主机. 如果移动主机的家乡代理接受到被封装的分组，这个封装分组的外部分组头没有路由头，则该分组按通常方式进行解封装. 如果内部分组头的目的地址不是 MAP，MAP 应该检查它的绑定缓存，看是否该地址是向它注册的移动主机之一. 如果是，该分组必须通过隧道发到移动主机注册的 LCoA；否则，该包被正常处理. 如果接收的封装分组有路由头，MAP 必须以通常方式处理路由头. 在处理路由头之后，MAP 必须检查是否最终目的地址与绑定缓存中的相一致. 如果是，MAP 必须通过隧道把分组发送到移动主机的 LCoA.

扩展模式对家乡代理的影响较小，唯一的影响是当使用站点本地地址通过隧道将分组发送到移动主机时，家乡代理应该在输出分组中包括路由头，以移动主机注册的全局家乡地址作为最终目的地址. 这是因为 MAP 不知道移动主机的家乡地址，通过使用路由头可以使 MAP 为移动主机找到正确的路由表项.

(2) 扩展模式对网络移动的支持

当移动主机也是一个路由器时，有几个移动主机与其相连. 在访问的网络中，该路由器可能无法获得新的网络前缀. 因此，与该路由器接连的移动主机将产生拓扑不正确的地址. 通过使网络中的移动路由器具有 MAP 的功能，连接到移动路由器的移动主机向家乡代理和通信对端进行注册时，可以使用移动主机的转交地址作为备用转交地址.

• 绑定更新

如果移动主机连接到一个移动路由器，路由器移动后可能无法获得拓扑正确的新网络前缀. 但是，移动主机还是希望以优化的路由保持与通信对端的通信. 在这种情况下，移动路由器(MR)既要作为一个路由器还要作为一个移动主机. 移动路由器要使用 IPv6 的无状态地址自动配置获得一个 LCoA，这个 LCoA 被连接到移动路由器上的移动主机用作它们的 RCoA.

如果移动主机不仅仅收到移动路由器发出的通告还收到更上层的 MAP 通告，移动主机对更上层的 MAP 的工作模式进行检查. 如果这个 MAP 工作在基本模式，则移动主机会使用此 MAP 的网络前缀形成自己的 RCoA. 然后，移动主机应该向移动路由器发送绑定更新包，将 RCoA 与它获得的地址进行绑定. 在发往到移动路由器的绑定更新消息中，源地址为移动主机的家乡地址，家乡地址域为 RCoA. 向 MR 的绑定完成后，移动主机向高层 MAP 发生绑定更新，消息中的家乡地址为移动主机的 RCoA. 如果 RCoA 被高层 MAP 拒绝，移动主机必须向移动路由器重发带有适当地址的绑定更新分组. 如果高层 MAP 操作在扩展模式，移动主机不需要向移动路由器 MR 发送绑定更新消息，因为移动路由器可以识别出移动主机与其同一个链路上. 为了能够接收路由优化的包，移动主机应该向高层 MAP 发送绑定更新分组，将它的家乡地址与移动路由器的转交地址进行绑定. 这将导致所有发送到移动主机的包转发到移动路由器，移动路由器接着将包转发到移动主机. 最后，移动主机必须向它的家乡代理发送以它的 RCoA 作为转交地址的绑定更新分组.

• 数据转发

如果 MAP 作为移动路由器，有一个或多个移动主机连接到它的一个接口上，并且 MAP 通过另一个接口连接在接入路由器上. 当 MAP 改变接入路由器时，MAP 必须通告它自己的 MAP 选项和从接入路由器接收到的其他 MAP 选项. 移动路由

器的 MAP 选项包含它自己的 LCoA．这将允许移动主机获得新的拓扑正确的 RCoA，并且向层次型结构中的高层 MAP 做绑定更新．如果高层 MAP 允许使用反向隧道，作为移动路由器的 MAP 应该将移动主机的分组通过隧道发送到高层的 MAP．

移动主机需要知道分组的最初发送者．当 MAP 工作在扩展模式下，MAP 通过隧道发送包，因此，移动主机不能直接决定分组是家乡代理通过隧道发送来的，还是直接从通信对端发送过来的．但是，移动主机需要知道这一情况，以决定是否需要向通信对端发送绑定更新消息，进行路由优化．因此，需要对内部分组的路由头进行检查，找到包是被家乡代理转发的，还是直接由通信对端发送的．如果内部分组的路由头存在，包括 RCoA，并且以移动主机的家乡地址作为最终目的地址，说明使用了路由优化；否则，就表示使用了通过家乡代理的三角路由．

4.3　一种新的 2 层签名算法

4.3.1　设计思想

本节提出的基于身份 2 层签名算法是根据文献[30]田等人提出的 2 层签名机制改进所得．在本算法中，每一层用户的私钥不再只依赖其父亲节点生成，而是由父亲节点以及自己的秘密参数分别生成的私钥部分组合而成．这种方法能更好地保证签名机制的安全性．同时，在验证部分，本算法能减少一次双线性对的运算，从而使效率有了一定的提高．

4.3.2　2 层身份签名机制

• 系统建立

根 PKG 生成阶为素数 q 的加法群循环 G_1 和乘法群循环 G_2．其中，$P\left(P \in G_1^*\right)$ 是 G_1 的生成元，$\hat{e}$ 是 $G_1 \times G_1 \to G_2$ 的一个双线性映射．根 PKG 随机选择整数 $s\left(s \in Z_q^*\right)$，计算 $P_{pub} = sP$．s 是系统私钥，P_{pub} 是系统公钥．选择杂凑函数 $H_1 : \{0,1\}^* \to G_1$，$H_2 : \{0,1\}^* \to Z_q^*$．系统建立后公开系统参数<$G_1, G_2, \hat{e}, P_{pub}, H_1, H_2$>．

• 密钥生成

系统第一层实体(PKG)的身份 ID 为一元组 I_1，随机选择整数 $s_1\left(s_1 \in Z_q^*\right)$，并且计算 $Q_1 = s_1 P$．根 PKG 计算 $P_1 = H_1\left(I_1\right) \in G_1$，并将 sP_1 发送给第一层 PKG．第一层 PKG 计算自己的私钥 $S_1 = sP_1 + s_1 P_1$．

系统第二层实体(用户)的身份 ID 为二元组(I_1, I_2)，随机选择整数$s_2\left(s_2 \in Z_q^*\right)$，并且计算$Q_2 = s_2 P$．第一层 PKG 计算$P_2 = H_1(I_1, I_2) \in G_1$，并将$S_1 + s_1 P_2$连同自己的$Q_1$发送给第二层用户．第二层用户计算自己的私钥$S_2 = S_1 + s_1 P_2 + s_2 P_2$．

• 签名

签名者对消息M进行签名：首先计算$P_M = H_2(I_1 \| I_2 \| M) \in Z_q^*$，然后计算$\sigma = P_M(S_1 + s_1 P_2) + s_2(P_{pub} + Q_1)$．

• 验证

验证者对签名值(σ, Q_2)的验证：验证者在收到签名之后，只要知道签名者父亲的Q_1值就可以通过下式来验证签名的真伪．

验证方程：$\hat{e}(P,\sigma) = \hat{e}(P_{pub}, P_M P_1 + Q_2)\hat{e}(Q_1, P_M P_1 + P_M P_1 + Q_2)$．

4.3.3 安全性分析

• 正确性验证

由本文 2.1 节介绍的双线性对的定义可得：

$$\begin{aligned}\hat{e}(P,\sigma) &= \hat{e}\left(P, P_M(S_1 + s_1 P_2) + s_2(P_{pub} + Q_1)\right)\\ &= \hat{e}\left(P, P_M(sP_1 + s_1 P_1 + s_1 P_2) + s_2(sP + s_1 P)\right)\\ &= \hat{e}\left(P, s(P_M P_1 + s_2 P) + s_1(P_M P_1 + P_M P_2 + s_2 P)\right)\\ &= \hat{e}(sP, P_M P_1 + s_2 P)\hat{e}(s_1 P, P_M P_1 + P_M P_2 + s_2 P)\\ &= \hat{e}(P_{pub}, P_M P_1 + Q_2)\hat{e}(Q_1, P_M P_1 + P_M P_2 + Q_2)\end{aligned}$$

• 不可伪造性证明

设用户的身份是 ID=(I_1， I_2)，私钥是$S_1 + s_1 P_2 + s_2 P_2$，针对消息M的签名<$\sigma \leftarrow P_M(S_1 + s_1 P_2) + s_2(P_{pub} + Q_1)$，$Q_2 \leftarrow s_2 P$>.

本节采用随机预言机模型证明改进的 2 层身份签名算法满足适应性选择消息攻击下的不可伪造性．

令敌手 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<G_1，G_2，$\hat{e}$，P，P_{pub}，Q_1，H_1，H_2，p，q>其中$q \geq 2^l$，$l = 160$．可以向用户发起n_1次签名查询，向随机预言机 H1 发起n_2次查询．

定理 4.1 若可以在时间t内以优势$\varepsilon \geq 10(n_1 + 1)(n_1 + n_2)/2^l$产生一个存在性伪

造签名，则存在另一个概率算法在时间$t' \le 120686n_2 t/\varepsilon$范围内解决$G_1$群上的APCDHP.

证明．根据文献[50-51]中的分叉引理，若可以在时间t内以优势$\varepsilon \ge 10(n_1+1)(n_1+n_2)/2^l$产生一个存在性伪造签名，则必然存在另一个概率算法，在时间$t' \le 120686n_2 t/\varepsilon$范围内产生两个有效签名$(M, Q_2, P_M, \sigma)$和$(M, Q_2, P_M', \sigma')$，其中$P_M \ne P_M'$.

基于构造一个概率算法.

令算法的输入为$<P, P_1, P_2, P_{pub}, Q_1>$，其中$P_1 = \alpha P$，$P_2 = \beta P$，$P_{pub} = sP$，$Q_1 = s_1 P$．随机选择一个消息$M$，运行算法，在时间$t' \le 120686n_2 t/\varepsilon a$范围内得到两个伪造签名$(M, Q_2, P_M, \sigma)$和$(M, Q_2, P_M', \sigma')$，其中$P_M \ne P_M'$．有

$$\hat{e}(P,\sigma) = \hat{e}(P_{pub}, P_M P_1 + Q_2) \times \hat{e}(Q_1, P_M P_1 + P_M P_2 + Q_2) \tag{4-1}$$

$$\hat{e}(P,\sigma) = \hat{e}(P_{pub}, P_M' P_1 + Q_2) \times \hat{e}(Q_1, P_M' P_1 + P_M' P_2 + Q_2) \tag{4-2}$$

将式(4-1)，(4-2)两式相除，得

$$\frac{\hat{e}(P,\sigma)}{\hat{e}(P,\sigma')} = \frac{\hat{e}(P_{pub}, P_M P_1 + Q_2) \times \hat{e}(Q_1, P_M P_1 + P_M P_2 + Q_2)}{\hat{e}(P_{pub}, P_M' P_1 + Q_2) \times \hat{e}(Q_1, P_M' P_1 + P_M' P_2 + Q_2)}.$$

$$\hat{e}(P,\sigma-\sigma') = \hat{e}(P_{pub}, (P_M - P_M')P_1) \times \hat{e}(Q_1, (P_M - P_M')(P_1 + P_2)),$$

$$\hat{e}(P,\sigma-\sigma') = \hat{e}(P, (sP_1 + s_1 P_1 + s_1 P_2)(P_M - P_M')),$$

$$\hat{e}(P,\sigma-\sigma') \times \hat{e}(P, (P_M - P_M')(sP_1 + s_1 P_1 + s_1 P_2))^{-1} = 1.$$

$$\hat{e}(P, (\sigma-\sigma') - (P_M - P_M')(sP_1 + s_1 P_1 + s_1 P_2)) = 1$$

令$(\sigma-\sigma') - (P_M - P_M')(sP_1 + s_1 P_1 + s_1 P_2) = \lambda P$，则式(4-1)得$\hat{e}(P,P)^{\lambda} = 1$，进而有$\lambda \equiv 0 (\mathrm{mod}\, q)$．因此，$(\sigma-\sigma') - (P_M - P_M')(sP_1 + s_1 P_1 + s_1 P_2) = 0 (\mathrm{mod}\, q)$，$sP_1 + s_1 P_1 + s_1 P_2 = (P_M - P_M')^{-1}(\sigma-\sigma')$其中$(P_M - P_M')^{-1}$表示$(P_M - P_M')$模$q$的乘法逆元.

最终，算法输出$sP_1 + s_1 P_1 + s_1 P_2 = (s+s_1)P_1 + s_1 P_2 = \alpha(s+s_1)P + \beta s_1 P$．根据之前的定义2.8，$G_1$群上的APCDHP就是给定$(P, aP, bP, cP, dP)$，其中$a$，$b$，$c$，$d \in Z_q'$输出$acP + bdP$．这就意味着算法在给定输入$<P, \alpha P, \beta P, P_{pub}, s_1 P>$的情况下，输出了$\alpha(s+s_1)P + \beta s_1 P$，即在时间$t' \le 120686n_2 t/\varepsilon$范围内解决了$G_1$群上的APCDHP．证毕.

4.4 基于身份的层次化移动 IPv6 切换技术

移动 IP 协议试图在网络层解决与节点移动性相关的所有问题，不借助下层协议的支持，同时保持对上层协议的透明性．在移动 IPv6 协议中，移动检测位置登记以及于此相关的安全问题等都在网络层解决，割裂了与上、下层之间的联系，既增加了切换延时，又使得安全保障强度不足．

移动 IPv6 网络中对服务质量的破坏主要来源于移动切换过程带来的延时和开销，以及由此对当前通信带来的丢包影响．对于移动节点来说，融合了接入认证的移动切换过程需要经历三个阶段：地址配置阶段、接入认证阶段和位置登记阶段．

身份密码学技术无论从部署还是密钥管理的角度来看，都比现有的 PKI 技术更简捷、方便．而且在身份密码学中，任何两个节点只要知道对方身份和一些辅助参数信息，就能很方便地进行有安全保护的通信，而不需要像 PKI 那样，每次通信前都必须向 CA 请求证书以及查询证书的有效性．利用身份密码学实现移动 IPv6 切换过程将从安全性和切换性能两个方面获得提高．

本协议中用到的符号说明如下：

ID_{MN}：移动节点 MN 的身份标识；

ID_{HA}：家乡代理 HA 的身份标识；

ID_{MAP}：外地代理 MAP 的身份标识；

BU_{MAP}：移动节点发往 MAP 的绑定更新消息；

BU_{HA}：移动节点发往 HA 的绑定更新消息；

MN_{CoA}：移动节点的转交地址；

MoA_{MN}：移动节点的组播地址；

$\{M\}_{Sign}$：对消息 M 的签名．

4.4.1 设计思想

移动节点 MN 通过接入路由器 AR 接入到移动子网，移动子网通过 MAP 接入公共网络．当 MN 移动到新的子网时，该网络的 MAP 为移动节点分配一个唯一的组播地址和转交地址．MN 在切换时，AR 根据链路层触发信息，构建组播树[52]．在组播树形成后，传送到 MN 的分组被传输到所有包含在组播树内的 AR 上，在上行方向上，MN 以单播方式向通信对端 CN 发送数据．

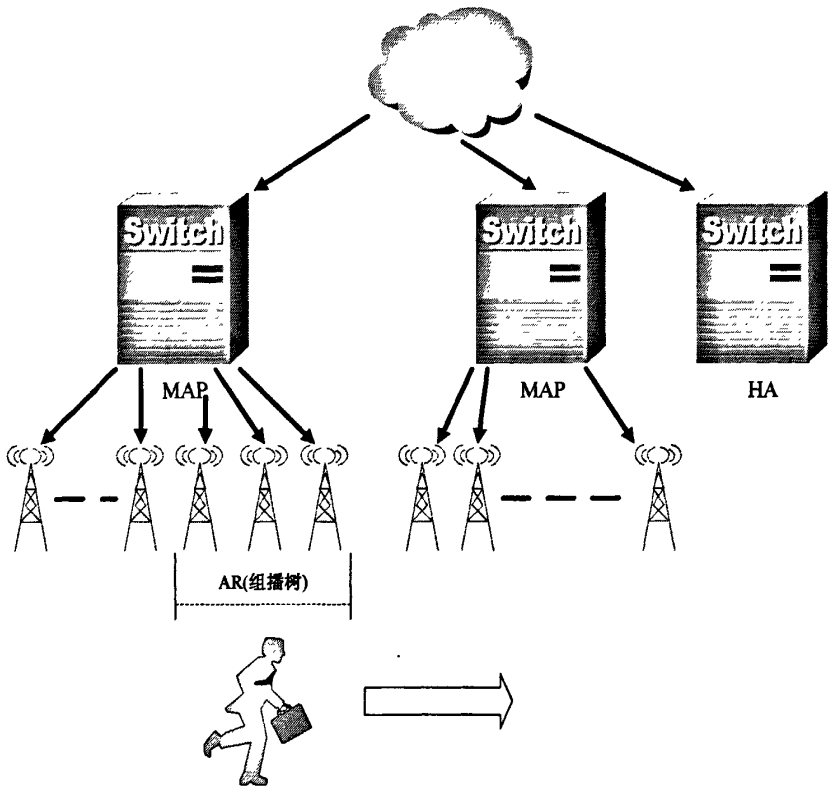

图 4.1　基于组播思想的层次化移动 IPv6 结构示意图

4.4.2　基于身份的层次化切换技术框架

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，AR 只需进行组播预定和组播删除操作即可．

(1)　MAP 域内的移动切换

具体描述如下：

(R1)　MN→nAR：M_1，$\{M_1\}_{Sign}$，ID_{MN}，Q_{MN}．

M_1 包括 Request，ID_{HA}，ID_{MAP}，MN_{CoA}，MoA_{MN}，T_{MN}．

当 MN 完成链路层切换，并获得链接连接成功信息后，通过注册信息将其组播地址告知 nAR．nAR 得到组播地址后，首先判断 MN 提供的组播地址是否为本子网的合法地址．如果是本子网的合法地址，则表明为 MAP 域内的切换．

nAR 将检索本地路由信息缓存以确定是否已加入相应的组播树．如果没有加入，则向网络内的组播路由器发出组播预订信息，将其自身加入组播树．此外，

nAR 还要发出组播成员删除消息，将其他 AR 从当前的组播树内删除．oAR 获取链路断开信息后，将退出当前的组播树．oAR 从链路层获得链路即将断开信息后，将向网络内的组播路由器发出组播预定消息，使其邻居列表内的 AR 都能加入针对 MN 的组播树．

MN 利用根 PKG 生成的公开参数和 HA 生成的Q_1，执行 4.3 节所提出的 2 层身份签名机制中的签名算法，生成对认证信息的签名以及自己的Q_2，一并发送给 nAR.

(R2) nAR→MAP：M_1，$\{M_1\}_{Sign}$，QVR.

nAR 首先查询自己的Q值列表，寻找是否存在I_1表项.

若存在，则直接取出对应的Q_1，结合得到的Q_2，执行 2 层身份签名机制中的验证算法验证$\{M_1\}_{Sign}$，同时检查时间戳T_{MN}，保证签名的新鲜性．当验证成功后，完成 nAR 对 MN 的认证.

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

(R3) MAP→nAR：

MAP 收到 QVR 消息后，查询存在I_1表项的Q值列表．因为 MN 在切换到 oAR 时，MAP 已经更新了 HA 的Q值(oAR 和 nAR 在同一个 MAP 域内)，所以一定存在这样的包含I_1表项的记录．此时，MAP 生成 QVA 消息将Q_1返回给 nAR.

(R4) nAR→MN：

nAR 使用Q_{MAP}和自己的私钥对绑定确认消息进行签名，并生成Q_{nAR}，然后将绑定确认消息连同签名以及Q_{MAP}、Q_{nAR}、$ID_{nAR}=(I_1^{'},I_2^{'})$组成回复消息.

验证 nAR 的签名，同时检查时戳T_{nAR}，保证签名消息的新鲜性．验证成功，则完成了 MN 对 nAR 的认证，实现双向认证.

(2) MAP 域间的移动切换

在域间移动切换的过程中，我们也采用 2 层身份签名机制对 MN 和接入网络实现双向认证．此时，认证框架需要进行如下的扩展.

(E1) 组播树的生成

在域内切换时，MN 的组播地址不变．而在域间切换时，当 nAR 发现 MN 发

送的组播地址并不是本子网合法的组播地址，nAR 并不将自己加入组播树．而在 MAP 为新加入的 MN 分配组播地址之后，nAR 加入组播树．

(E2)　获取 HA 的Q值

在域间切换时，nAR 和 MAP 并没有 HA 的Q值，此时 MAP 需要向 HA 询问Q值．同时，HA 也需要对 MN 的转交地址进行注册绑定，此过程与传统的层次化移动IP协议一致．此时认证过程的消息流则可表示为：MN→nAR→MAP→HA→MAP→nAR→MN．

(E3)　对 MAP 的认证

在域间切换的过程中，需要增加 MN 对 MAP 的认证．MAP 在返回注册消息时，用Q_{MAP}对发送的消息进行签名．MN 在验证 nAR 的签名之前，还需要验证 MAP 的签名．

4.5　安全性和切换延时分析

下面我们基于集中攻击模型对于新协议进行安全性分析．在效率分析方面，我们主要分析了新方案对切换延时的改进．

4.5.1　安全性分析

(1)　协议对于拒绝服务攻击是安全的

攻击者用自己的 IP 地址来冒充注册者的转交地址，从而用伪造的注册请求信息来进行注册．一旦攻击者攻击成功，敌手将能够得到通信对端发送的数据．攻击者用自己的 IP 地址来冒充注册者 MN 的组播地址或者转交地址，但是却不能生成消息的签名．如果攻击者首先伪造签名值，则不可能得到其对应的消息．

攻击者没有签名者的私钥．在基于身份的密码体制中，签名与验证双方的公钥采由节点的身份(一般为身份的哈希值)，而私钥则为 PKG 生成．这样大大降低了密钥管理的难度．在文献[30]中所提出的 2 层身份签名机制中，第一层 PKG 的私钥由根 PKG 生成，第二层用户的私钥由第一层 PKG 生成．于是，用户节点的父亲则可以伪造该实体的签名或监听该实体加密通信．而在本文 4.3 节提出的 2 层身份签名机制中，每一层实体的私钥均由父亲节点和自己共同生成(根 PKG 除外)．并且这种机制具有很好的扩展性，第i层实体的私钥$S_i = S_{i-1} + s_{i-1}P_i + s_iP_i$．其

中，$s_i \in Z_q^*$为第i层实体随机选择并秘密保存．这样做的好处是，实体的私钥只有自己可以生成，很好的保证了数据的机密性．同时，在认证过程中，攻击者同样不能伪造出用户的签名．

攻击者也可能会截获由 AR 返回 MN 的注册回复信息，使得 MN 不能注册成功．当注册节点遭到此类攻击，即在注册请求发出后预定时间内未能收到注册回复消息的情况下，重新生成注册信息和签名，重新发送．

(2) 协议对于重放攻击是安全的

针对移动 IP 协议的重放攻击也包括两种：攻击者向 HA 或者 CN 重新发送注册请求消息．

攻击者截获并保存一个先前已经被 HA 或者 CN 成功接收的注册请求消息．等到移动节点离开该 MAP 后，攻击者向 HA 重新发送该请求消息，以便把发送给 MN 的数据包仍然定向到以前所处的位置．

MAP 向 HA 发送的注册请求中包括发送消息时的时戳T_{MAP}，而该消息还附带有 MAP 的数字签名，故攻击者不能更改请求消息中的时戳．HA 在收到请求消息后，需要查看消息中附带的时戳，已确保消息的新鲜性．所以，本协议可以抵御此类攻击．

(3) 协议对于中间人攻击是安全的

在层次化移动 IPv6 中，中间人攻击是指，攻击者假冒中间人 AR 或者 MAP 来窃取 MN 和 HA 之间的注册信息．

首先，MN 进行域内切换时协议对于 AR 的中间人攻击是安全的．本协议中完成了 AR 和 MN 的双向认证．在 AR 的注册应答中包含自己的Q_{nAR}，这样 MN 就可以通过Q_{MAP}、Q_{nAR}来验证 AR 的 2 层签名，来确认 AR 的身份．

其次，对于域间切换 MAP 在收到注册节点的注册请求消息之后，增加外地家乡代理之间的认证扩展，并且对发往 HA 的消息进行签名．MAP 增加的认证扩展中包括 MAP 的证书$Cert_{FA}$.HA 可以在获取 MAP 的证书之后来验证 MAP 的签名，以实现对 MAP 的认证．所以，协议对于中间人攻击是安全的．

(4) 协议对于被动攻击是安全的

被动攻击分为以下两种：窃听链路上传输的密钥等秘密信息、窃听 MN 的身

份信息.

在本协议中，任何一个第二层用户的私钥均是由父亲节点发送的$S_1 + s_1 P_2$和自己的秘密参数s_2计算所得．尽管用户私钥是由父亲节点的私钥加上$s_1 P_2 + s_2 P_2$得到的，但是由于用户不知道父亲节点的秘密参数s_1，所以不能由$S_1 + s_1 P_2$计算出父亲节点的私钥．同样，由于父亲节点不知道用户的秘密参数s_2，所以也不能计算出用户的私钥．同理，网络中的其他节点不能计算得到用户的私钥，由链路上窃听得到的信息也不能得到用户的私钥.

4.5.2　切换时延分析

移动 IP 切换时延主要是指移动主机在切换时的 IP 层时延，即移动主机从收到来自新访问域的第一个路由宣告消息包到收到绑定更新完成通告之间的这段时间.

IP 层时延主要包括以下几个部分：移动检测时延T_{MD}和移动注册时延T_{REG}．移动注册时延分为以下三个部分：获取转交地址的时延T_{CoA}、重复地址检测时延T_{DAD}和绑定过程中的时延T_{BU}.

对于绑定过程中产生的时延我们从以下两个角度来分析，一是绑定消息传输时延和本机消息处理时延，另一类是绑定消息认证算法执行时节点所用的时延.

(1)　从切换机制的角度分析时延

为了改善移动 IPv6 的切换性能减小切换时延，IETF 公布为草案的方案有：快速切换技术和层次化移动 IPv6.

快速切换技术在与旧接入路由器*oAR*保持连接的情况下，发起切换或者预先建立和新接入路由*nAR*的联系．快速切换技术可以省去重复地址检测时延T_{DAD}，其余部分和传统的移动 IPv6 协议一致．然后在移动节点远离家乡代理时，认证信息的交互在与家乡代理的传输过程中时延变大．特别是在需要频繁切换时，层次化移动 IPv6 就表现出自己的优点.

层次化移动 IPv6 中移动节点的切换分为两种，MAP 域内的切换和 MAP 域间切换．对于远离家乡代理的节点，MAP 域内切换大大的降低了切换时延．移动节点只需要在 MAP 处注册自己的本地转交地址．而在域内的切换过程对于家乡代理是完全透明的．但是要指出的是，在 MAP 域间的切换时延要远远低于普通的移动

IPv6 协议.

而本文提出的切换机制，在 MAP 域内采用统一的组播地址，避免了注册本地转交地址的时延. 旧接入路由器在链路层获得链路即将终止信息时，即向 MAP 发送组播预定消息，使其邻居列表内的 AR 都能够加入针对 MN 的组播树，从而避免了域内切换的时延.

从认证机制的角度来看，本文采用的 2 层身份签名机制只需要 MN→AR→MAP(→HA)的一次交互就可以完成移动节点和接入路由器的双向认证. 文献[53]中采用的认证过程基于挑战-应答方式，需要 MN 和家乡域的认证服务器的多次交互，若要实现双向认证需要来回交互三次. 而文献[54]中提出的 HAMIPv6 协议尽管使用了捎带挑战字，但也需要交互两次来实现双向认证.

(2) 从认证算法的角度分析时延

从上一段的分析我们看出，2 层身份签名机制和文献[53]、文献[54]中的切换机制相比在消息交互时延方面有很大的优势. 但是与此同时，付出的代价是执行认证算法时的时延较高. 由文献[30]的分析我们可以得出结论，当节点处理认证时延较低和访问域距家乡域路程较长的情况下，2 层身份签名机制有着绝对的优势.

在这里我们分析文献[30]中的2层身份签名机制和本文所提出的改进方案在时延方面的比较. 在签名时，本文的 2 层身份签名需要进行一次哈希运算，两次加法和两次乘法运算，文献[30]中的方案则需要哈希运算，加法运算和乘法运算各一次. 但是在验证的过程中，本文的 2 层身份签名只需要三次双线性对运算和一次乘法运算，文献[30]中的方案则需要四次双线性对运算和两次乘法运算. 相对于双线性对运算，加法和乘法运算的运算则非常的小. 所以和文献中的 2 层签名算法比较，本文的改进算法在提高了私钥机密性的基础上验证计算方面效率也得到了提高.

综上可知，本文所提出的协议不仅有很好的安全性，效率也有了显著的提高，并且更具有实用价值.

4.6 本章小结

上一章对于移动 IP 注册协议，主要是从认证的角度来研究的. 本章研究移动 IP 的切换技术，我们不仅研究了认证机制，而且包括切换管理机制. 本章提出了一个基于身份的层次化移动 IP 切换技术. 其中的接入认证部分采用改进的 2 层身份签名机制，本章提出的切换机制在层次换移动 IP 的基础上，加入了组播的思想. 使得移动节点在 MAP 域内切换的效率更高. 经过分析，该方案在安全性和效率方面都有了一定的提高.

第五章　总结与展望

移动 IP 技术是下一代网络中一种重要的技术．三网融合的进一步推进，各种无线技术的风起云涌，使得人类实现“在任何时候任何地点，用任何一种媒体和任何一个人进行通信”的梦想即将成为现实．移动通信和互联网技术的迅猛发展，使得移动互联的需求更加迫切．也正是由于这种契机，移动 IP 技术从众多的移动通信技术中脱颖而出，成为越来越多研究机构和标准化组织关注的焦点．

移动互联网技术的发展将使人们的生活方式发生重大的改变．也许在不久的将来，我们就可以在去机场的路上用手机办理签证和银行业务，在旅行的途中用 ipad 参加公司召开的紧急视频会议．这一切的前提是我们办理的所有这些业务必须安全，可靠．无线通信由于自身传输介质等方面的特点，安全性保证相对比较薄弱．在目前语音业务所占比重较大的今天尚不足以为患，然而在不久的将来移动互联网技术要大力推进必须首先解决安全问题．

本文从安全的角度分别研究了移动 IP 注册协议和移动 IP 切换技术．首先介绍了移动 IP 技术产生和应用的背景，概述了国内外研究现状，并且对移动 IP 协议的框架做了简单介绍；接着，介绍了本文研究所需的各种预备知识．

对于移动 IP 注册协议的研究，第三章详细描述了本文在该领域的研究成果．在移动 IP 注册协议中，认证的安全性和效率也决定了注册协议的安全性和效率．在不安全的无线信道中使用对称密码技术很难设计出安全可靠的认证方案．此外，当网络规模急剧增大时，为每一对需要通信的用户分发密钥，在密钥管理上难度很大．而基于证书的公钥密码技术虽然能够很好的解决这一问题，但是需要移动节点的计算开销却很大，不太适合在实际中应用．本文第三章提出的移动 IP 注册协议采用基于身份公钥密码体制，用一种新的密钥协商方式将认证所需的计算量转嫁到移动代理，而不是计算能力、存储能力和能量均有限的移动节点，从而提高了效率．

对于移动 IP 切换技术的研究，目前针对各种应用已经提出了众多的方案．作为 IETF 颁发的标准(草案)，层次化移动 IP 技术对移动 IPv6 协议进行了扩展，提高了切换效率．本章提出的切换技术是在层次化移动 IP 的基础上，加入了组播的思想，用组播地址代替层次化移动 IP 技术中的本地转交地址．这样，在本地域中切换时的效率就能大大提高，同时也避免了完全采用基于组播的切换技术网络负载量大的缺陷．在第四章我们采用了改进的 2 层身份签名机制，提出了一套集注册认证，切换技术于一体的完整解决方案．

由于时间和能力有限，作者虽然做了一定的工作，但还留下以下问题有待进

一步探索和研究：

(1) 本文对协议的分析中只从安全性和计算效率的角度进行分析，在今后的方案设计中可以综合考虑各种因素，不仅能使安全性、计算效率得到提高，在丢包率和平滑等方面也应该有所改进.

(2) 本文的协议安全性证明可以考虑采用形式化语言证明.

(3) 设计新的效率更高的移动 IP 协议，以及研究该协议在现有各种网络中的实际应用问题.

由于作者的水平有限，论文中的不足之处在所难免，敬请各位评审专家和读者批评指正!

致 谢

首先感谢我的导师马华老师．本文是在马华老师的悉心指导下完成的．在两年半的学习和研究过程中，马老师为我们创造了良好的学习环境．马老师知识广博，管理上宽松自由，细节上认真严谨．她学习上对我们严格但又不失和蔼的态度，生活上无微不至的关心都给我留下了深刻的印象．我的工作主要是协议的设计，而她在这方面的对我的指导，更让我受益匪浅．

感谢王保仓老师、党岚君老师，论文的完成离不开王老师悉心的指导和帮助．感谢他们在平时给我的指导．

感谢同门的张凤荣博士、刘光军博士、张应辉博士、黄玉颖硕士等在学习过程中给予的支持和帮助，与他们就科研问题的讨论让我获益良多，向他们表示由衷的敬意和感谢．感谢我的舍友李云红、张成才以及07081班的所有兄弟姐妹们，能在这样一个充满友爱和智慧的集体里学习和生活，使我深感幸运，与他们相处的每一天都给我留下了美好的回忆．

最后，我要特别感谢辛勤养育我多年的父母．在我成长过程中的每一步，都离不开他们的关心与支持．特别是对于一直都关心着我的母亲和姐姐，我不能陪在她们身边照顾她们，她们对我的爱我无以为报．

仅借此机会向所有给予我关心、支持和帮助的人们表示由衷的感谢！

参考文献

[1] 孙利民，阚志刚，郑健平等．移动IP技术[M]．北京：电子工业出版社，2003年8月．

[2] 周贤伟，景晓军，覃伯平等．移动IP与安全[M]．北京：国防工业出版社，2005年9月．

[3] 蒋亮，郭健．下一代网络移动IPv6技术[M]．北京：机械工业出版社，2005年6月．

[4] 张玉军．可信的移动IPv6网络及协议[M]．北京：科学出版社，2008年3月．

[5] Perkins C. IP Mobility Support. IETF RFC2002, Oct., 1996.

[6] Perkins C. IP Encapsulation within IP. IETF RFC2003, Oct., 1996.

[7] Perkins C. Capsulation within IP. IETF RFC2004, Oct., 1996.

[8] Solomon J. Adaptability Statement for IP Mobility Support. IETF RFC2005, Oct., 1996.

[9] 党岚君．移动IP安全注册协议研究[D]．西安电子科技大学博士论文，2008年9月．

[10] Perkins C. IP mobility support for IPv4. IETF RFC3220, Jan., 2002.

[11] Perkins C. IP mobility support for IPv4(obsoletes 3220).IETF RFC3344, Aug., 2002.

[12] 王育民，刘建伟．通信网的安全——理论与技术[M]．西安：西安电子科技大学出版社，1999年4月．

[13] Zao J, Kent S, Gahm J, et al. A public-key based secure mobile IP[J]. Wireless Networks, 1999, 5(5): 373-390.

[14] Jacobs S. Mobile IP public key based authentication[DB/OL]. [2010-09-20]. http://www3.ietf.org/proceedings/99mar/slides/mobileip-key-99mar.pdf.

[15] Yoo J P, Kim K, Choo H, et al. Secure and scalable mobile IP registration scheme using PKI[C]. ICCSA 2003, LNCS 2668. Berlin:Springer-Verlag, 2003: 220-229.

[16] Qian H Y, Chen B, Qin X L. A novel mobile IP protocol supporting roaming subnet[C]. 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009:274-277.

[17] Yong L, Goo Y L, Hwa J K. Design and performance evaluation of a scalable authentication protocol in mobile IP[C]. Second International Conference on Communications and Networking in China, 2007:1069-1074.

[18] Sufatrio, Lam K Y. Mobile IP registration protocol: a security attack and new secure minimal public-key based authentication[C]. Proceedings. The Fourth International Symposium on Parallel Architectures, Algorithms, Algorithms, and Networks 1999, 1999: 364-369.

[19] Chung S, Chae K. An efficient public-key based authentication with mobile IP in E-commerce[C]. Proc. IEEE Int. Conf. On Parallel and Processing 2000, 2000.

[20] Yang C C, Huang M S, Li J W, et al. A solution to mobile IP registration for AAA[C]. LNCS 2524: CIC 2002. Berlin: Springer-Verlag, 2003: 329-337.

[21] Mufti M and Khanum A. Design and implementation of a secure mobile IP protocol[C]. International Networking and Communication Conference 2004, 2004: 53-57.

[22] Yang C Y and Shiu C Y. A secure mobile IP registration protocol[J]. International Journal of Network Security, 2005, 1(1): 38-45.

[23] Dang L J, Kou W D, Li H, Zhang J W, et al. Cost analysis of IP mobility management protocols for consumer mobile devices[J]. IEEE Transactions on Wireless Communications,2010, 9(2): 594-605.

[24] 赵庆林，张玉军. 增强移动IP性能的快速切换技术综述[J]. 计算机工程，2005，31(7)：3-4.

[25] 方波，宋俊德. 移动IP切换技术研究[J]. 大连理工大学学报，2003，43(supp. 1)：30-33.

[26] Soliman H, Castelluccia C, Elmalki K, et al. Hierarchical mobile IPv6 mobility management. IETF RFC5380, Oct., 2008.

[27] Koodli R. Fast handovers for mobile IPv6. IETF RFC4068, July, 2005.

[28] Tie L, He D, Li J H, Tang J H. Performance analysis of authentication method for Proxy Mobile IP protocol[C]. The 2nd International Conference on Biomedical Engineering and Informatics, 2009:1-4.

[29] Lee J H, Ernst T, Chung T M. Cost analysis of IP mobility management protocols for consumer mobile devices[J]. IEEE Transactions on Consumer Electronics, 2010,56(2):1010-1018.

[30] 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.

[31] Boneh D, Frankin M. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computing, 2000,32(3): 586-615.

[32] Shamir A. Identity-based cryptosystems and signature schemes[C]. Proc of the Advances in Cryptology Cryptop84. Berlin: Springer, 1984:47-53.

[33] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Trans. On Information Theory, 1976, 22(6): 644-654.

[34] 沈昌祥，张焕国，冯登国等. 信息安全综述[J]. 中国科学，2007，37(2)：129-150.

[35] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. IETF RFC3775, June, 2004.

[36] Solomon J D著，裘晓风等译. 移动IP. 北京：机械工业出版社，2000年.

[37] 袁宏伟，胡修林，张蕴玉. 移动IP及其信息安全[J]. 移动通信. 2003，3：44-46.

[38] W. Mao. Modern cryptography: theory and practice[C]. One Lake St., Upper Saddle River, NJ: Prentice Hall, 2004: 364-367.

[39] 崔海燕. 移动IP中几个安全问题研究[D]. 西安电子科技大学硕士论文，2005年1月.

[40] 王晓涓，陈淑静. 移动IP的被攻击形式及解决方案[J]. 天中学刊. 2004，19(5)：44-45.

[41] Choi D H, Kim H, Jung K. A secure mobile IP authentication based on identication protocol[C]. Proceedings of 2004 International Symposium on Intelligent Signal Processing and Communication Systems, 2004: 709-712.

[42] Perkins C, Calhoun P. Mobile IPv4 challenge/response extensions. IETF RFC3012, Nov., 2000.

[43] 朱建明，马建峰. 一种高效的具有用户匿名性的无线认证协议[J]. 通信学报，2004，25(6)：12-18.

[44] 彭华熹，冯登国. 匿名无线认证协议的匿名性缺陷和改进[J]. 通信学报，2006，27(9)：78-85.

[45] 张胜，徐爱国，胡正明等. 基于身份公钥的移动IP认证方案[J]. 北京邮电大学学报，2005，28(3)：86-88.

[46] 党岚君，寇卫东，曹雪菲等. 具有用户匿名性的移动IP注册协议[J]. 西安电子科技大学学报，2008，35(2)：282-287.

[47] 马华，任伟超，党岚君等. 基于身份的移动IP注册协议[J]. 北京工业大学学报，2010，36(supp. 2)：123-127.

[48] Smart N P. An identity based authenticated key agreement protocol based on the Weil pairing[J]. Electronics Letters, 38(13): 630-632.

[49] Paulo S L M B, Hae Y K, Ben L, et al. Efficient algorithms for pairing-based cryptosystems[C]. Yung M, LNCS 2442: CRYPTO 2002. Berlin: Springer-Verlag, 2001: pp. 354-369.

[50] Pointcheval D, Stern J. Security proofs for signature scheme[C]. Advances in Cryptology Eurocrypt 1996. LNCS1070. Heidelberg: Springer-Verlag, 1996:

387-398.

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

[52] 俞一帆，记红，乐光新．一种基于组播的移动IP跨层切换机制[J]．北京邮电大学学报，2006, 29(6): 125-128.

[53] Le F, Patil B, Perkins C, et al. Diameter mobile IPv6 application. Draft-le-aaa-diameter-mobileeipv6-04.txt Internet Draft, Nov. 2004.

[54] Engelstad P, Haslestad T, Paint F. Authenticated access for IPv6 supported mobility[C]. Proceedings the Eighth IEEE International Symposium on Computers and Communication 2003, 2003: 569-575.

硕士期间论文发表情况及科研工作

一 论文发表情况

[1] 马华，任伟超，党岚君，王保仓．基于身份的移动 IP 注册协议．北京工业大学学报，2010，36(Supp.2)：123-127．(EI number：20104513372710)

[2] 任伟超，黄玉颖，董博．一种基于组播的层次化移动 IPv6 切换技术．西安电子科技大学 2010 年研究生学术年会理学院数学系论文集．

[3] 黄玉颖，任伟超，史来婧．基于身份的强指定多个验证者签名方案．西安电子科技大学 2010 年研究生学术年会理学院数学系论文集．

二 参与的科研工作

1. 国家自然科学基金青年基金项目《后量子背包公钥密码的新型设计与差分分析》(60803149).
2. 中国电子科技集团公司第五十四研究所与高校合作项目：无线快速移动无中心自组网络抗毁、抗干扰及信息安全技术研究．