移动计算网络中代理主机的认证协议

李玉林，董雨果，李祖鹏，郑连清
(空军工程大学 电讯工程学院，陕西 西安 710077)

摘　要：首先讨论认证协议所要满足的安全要求和技术要求，并在此基础上设计一种移动计算网络中代理主机的认证协议。该协议基于公钥体制实现双向认证，安全性好且运行效率高。

关键词：移动计算网络；移动代理主机；认证
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-3516(2001)02-0034-03

随着移动计算网络(MCN-Mobil Computing Networks)的逐步成熟，安全认证技术变得愈来愈重要。迄今为止，人们为移动通信系统设计了许多认证协议[1~3]，然而这些协议并不能很好的满足MCN发展的需求，其中存在的问题可概括为：

- 基于私钥体制[1~3]，要求移动主机、代理端、网络端等认证实体产生并保存数量庞大的密钥。
- 认证信息交互次数多[1]，因而遭受安全攻击的可能性较大，也容易造成信道繁忙。
- 依靠于安全认证的传递性[2,3](即A相信B，B又相信C，所以A相信C)，无法防止来自网络内认证实体的联合攻击，而且不能明确划分安全的管理责任。

在MCN中由某一移动主机指定作为其代理的一位或多位其它移动主机称为移动代理主机(MPH-Mobile Proxy Host)。对MPH的认证可分为：MPH在本地网的认证及MPH漫游时的认证。前种情况较简单，本文主要讨论MPH在网络层漫游时的认证问题。

1　设计要求

在网络上实现信息的安全传输涉及到OSI模型的每一层，本文仅讨论网络层。协议要求可分为安全要求和技术要求。

1.1　安全要求

- 双向认证，即MPH与MH之间的相互认证，以及MPH、MA和HA之间的相互认证；
- 信息的保密性，即要求有可靠的加密算法和抵抗重放攻击的能力；
- 充分保护每个实体的私钥；
- 不可抵赖性，即要求收发双方不能否认自己所发出和接收的信息。

1.2　技术要求

- 对用户主机透明；
- 传递的数据尽量少。因为MPH漫游时将跨越低速广域网络，传送大量的数据很费时；
- 与MCN中其它安全协议的相融性。

2　MPH认证协议

首先给出与本协议有关的几个概念。

2.1　概念

收稿日期：2000-06-13
基金项目：国家自然科学基金资助项目(69631020).
作者简介：李玉林(1973-)，男，湖南衡山人，硕士生，主要从事移动通信方面研究.

•代理证明:代理证明由原签名者生成,它含有原签名者的私钥和代理签名者的公钥。
•代理密钥:代理密钥由代理签名者的私钥和原签名者的代理证明构成,它用来生成代理签名。
•代理签名:用代理密钥生成的数字签名。通过对它的验证可同时认证原签名者和代理签名者。
•代理公钥:代理公钥由原签名者和代理签名者公钥生成。它用来验证代理签名。

2.2 协议的描述

假定本协议采用 ITU-T 的 X.509 公钥认证机制,每个实体利用身份证号 ID 可安全地获得其它实体的公钥。另外,本协议不特别指明数字签名及验证签名的算法,MCN 系统可根据具体需要选取适当的算法。

为了便于描述,首先对相关的参数和符号作如下说明:

•系统中的公开参数:p,q。其中 p 是一个素数模且 $2^{1023}<p<2^{1024}$;g 是 GF(p)中阶为 $p-1$ 的一个生成元。
•MH 具有两对密钥:私钥 s_{MN},公钥 R_{MN}及另一私钥 k_{MN},公钥 L_{MN};MPH 具有一对密钥:私钥 R_{MPH},公钥 R_{MPH};实体的公钥 R 与私钥 s 满足以下关系:

$$R = g^s \bmod p \tag{1}$$

•C_{MH}:MH 生成的代理证明。
•ps:MPH 生成的代理密钥。
•PR:代理密钥 ps 对应的代理公钥。•$Sig_{ps}(x)$:MPH 对消息 x 生成的代理签名。
•$Sig(x)$:实体 i 对消息 x 生成的普通签名。
•n·FA 生成的一次性随机数(nonce)。
•m·MPH 生成的一次性随机数。
•ID_{MPH}:MPH 的标识。

下面是对协议的详细描述,该协议分为两个阶段:

2.2.1 代理指定阶段

•MH 通过下式生成代理证明 C_{MH}

$$C_{MH} = s_{MH} + k_{MH}R_{MPH} \bmod p - 1 \tag{2}$$

•MH 向 MPH 发出 C_{MH},
•MPH 通过下式验证 C_{MH},

$$g^{C_{MH}} = R_{MH}L_{MH}^{R_{MPH}} \bmod p \tag{3}$$

如果上式不成立,则 MPH 拒收 C_{MH};终止协议;反之,MH 得以认证;
•MPH 向 MH 发出签名 $Sig_{MPH}(C_{MH})$;
•MH 验证 $Sig_{MPH}(C_{MH})$可实现对 MPH 的认证。

至此,MH 已成功地指定 MPH 为其合法代理。

2.2.2 漫游 MPH 的认证阶段

•当 MPH 漫游时,MPH 收到访问网络广播的区域标识信息,MPH 判断出漫游服务状态;
•MPH 向 FA 发出漫游服务请求,其中包括 MPH 的标识 ID_{MPH},
•FA 利用收到的请求判断出漫游服务状态,并利用 ID_{MPH}得到 MPH 的公钥 R_{MPH}和 MH 的公钥 R_{MN}及 L_{MN}。FA 生成一次性随机数 n,并向 MPH 发出 n;
•MPH 通过下式生成代理密钥 ps:

$$ps = C_{MH} + s_{MPH} \bmod p - 1 \tag{4}$$

然后 MPH 生成一次性随机数 m,最后向 FA 发送代理签名 $Sig_{ps}(n,m,C_{MH})$;
•FA 通过下式生成代理公钥 PR

$$PR = R_{MH}L_{MH}^{R_{MPH}}R_{MPH} \bmod p \tag{5}$$

FA 用 PR 对代理签名进行验证,如果验证成功,则可以认证 MPH 为 HA 的合法代理;否则,终止协议。FA 向 HA 发送两重签名 $Sig_{FA}(Sig_{ps}(n,m,C_{MH}))$;
•HA 通过验证此双重签名可以认证 FA 及 MPH。HA 向 FA 发送签名 $Sig_{HA}(m,n)$;
•FA 通过验证签名 $Sig_{HA}(m,n)$可以认证 HA。FA 向 MPH 发送两重签名 $Sig_{FA}(Sig_{HA}(m,n))$;
•MPH 利用两重签名 $Sig_{FA}(Sig_{HA}(m,n))$便可完成对 HA 和 FA 的认证。

至此,漫游 MPH 的认证协议已完成。

3 协议的性能分析

3.1 安全性分析

- 双向认证:移动通信中,双向认证的目的是鉴别认证实体身份,防止假冒实体的攻击。假冒实体的通用攻击手段包括:

  a)获取合法实体的私钥或认证密钥。

  b)重放攻击,即利用合法实体以前使用过的信息进行非法访问。

  假冒实体可能对传输的签名信息进行分析,解出密钥。这种可能性取决于加解密算法的安全性,本文假定协议所采用的加解密算法具有足够高的安全性。协议中的一次性随机数 m、n 用于抵抗重放攻击。
- 不可抵赖性:如果 MPH 否认 FA 向他(她)提供过漫游服务,FA 可将代理签名 $Sig_{ps}(n,m,C_{MH})$ 作为证据交由共同信赖的第三方进行仲裁,因为用于签名的代理密钥 ps 含有 MPH 的私钥 s_{MPH},只有 MPH 才能生成合法的 ps,别的实体甚至包括 HA 都不能够伪造出 ps,所以 MPH 无法抵赖曾接受 FA 的服务。

3.2 运行效率分析

- 传输数据量:在漫游 MPH 的认证协议中,MPH 与 FA 间需要传输一次随机数,一次普通签名和一次两重签名;FA 与 HA 间需要传输一次普通签名和一次两重签名。
- 交互过程:可以看出,FA 与 HA 只需要一次交互过程便可完成相互认证;MPH 与 FA 之间也只需一次交互过程,这同时也实现对用户主机透明。

4 结束语

本文基于代理签名设计一种 MCN 中代理主机的认证协议。分析表明,该协议安全性好,运行效率较高。MCN 的发展对认证技术提出很多新要求,在 MCN 的安全认证技术中应用公钥体制是一个崭新的课题,相关的一些问题(如公钥管理系统的建立及公钥的分配机制)还需要进一步研究。

参考文献:

[1] Suzuki Shigefusa, Nakada Kazuhiko. An Authentication Technique Based on Distributed Security Management for the Global Mobility Network[J]. IEEE Journal on select, 1997, 12(7): 1208 - 1217.

[2] Liu Jianwei, Wang Yumin. A User Authentication Protocol for Digital Mobile Communication Network[A]. 7th IEEE International Symposition on Personal, Indoor and Mobile Radio Communications, Beijing, China · PIMRC'96. 1996 · 1239 - 1242.

[3] 高京力,郭 峰,黎长安. 移动计算网络中漫游主机的认证协议[A]. 中国通信学会. 1997 通信学术交流会议集[C]. 北京:电子工业出版社,1997. 19 - 23.

[4] Seungjoo Kim, Sangjoon Park, Dongho Won. Proxy Signatures, Revisited[A]. ICICS97 · 223 - 232.

[5] 周保太,季庆光. 公钥密码体制发展的一种新方向:代理密码体制(I)[J]. 密码与信息,1998,5(3):1 - 21.

A Protocol for Authentication of Mobile Proxy Hosts in Mobile Computing Networks

LI Yu - lin, DONG Yu-guo, LI Zu-peng, ZHENG Lian-qing

(The Telecommunication Engineering Institute of the Air Force Engineering University (AFEU.), Xi'an 710077, China)

Abstract · In this paper, the security and technique requirements of protocols for authentication are given, and a protocol for authentication of mobile proxy hosts in mobile computing networks is proposed. Based on the public key cryptosystems, the protocol implements mutual authentication and is of high security and efficiency.

Key words · mobile computing network; mobile proxy hosts; authentication