◎网络、通信、安全◎

一种移动互联网络匿名认证协议

张 婕,吴振强,霍成义,见晓春
ZHANG Jie,WU Zhen-qiang,HUO Cheng-yi,JIAN Xiao-chun

陕西师范大学 计算机科学学院,西安 710062
College of Computer Science,Shaanxi Normal University,Xi'an 710062,China

ZHANG Jie,WU Zhen-qiang,HUO Cheng-yi,et al.Anonymity authentication protocol in mobile Internet.Computer Engineering and Applications,2008,44(13):80-83.

Abstract: According to anonymous request of mobile internet security.An identity-based cryptography mutual authentication protocol is proposed to resolve the problem of identity authentication and key agreement in mobile communication,It can provide anonymous service that guarantees the confidentiality of the mobile users' identity.The research results reveal that the protocol has a good anonymous property,and is efficient and feasible and achieves the ideal security requirements of anonymity for Wireless Mobile Internet.

Key words: anonymit;identity authentication;key agreemet

摘 要:针对移动互联网络安全性的匿名需求,论文在基于身份的公钥系统的基础上,设计了一个双向匿名认证协议,该协议提出移动互联网络通信中的匿名身份认证和密钥协商方案,实现了通信双方的相互认证,并使移动网络向移动用户提供匿名服务,保护用户身份信息,分析表明协议具有很强的匿名性,而且高效可行,满足移动互联网络匿名性的安全需求。

关键词:匿名;身份认证;密钥协商
DOI:10.3778/j.issn.1002-8331.2008.13.024 **文章编号**:1002-8331(2008)13-0080-04 **文献标识码**:A **中图分类号**:TP393.08

1 前言

随着信息网络技术的快速发展,尤其是一些新型网络技术的不断出现,人们不再满足于使用固定终端或单个移动终端连接到互联网络上,而是希望移动子网络(如运动中的军队、航天中的飞行器、航行中的轮船、移动中的汽车和火车等运动主体上的网络)也能以一种相对稳定和可靠的形式,从 Internet 上动态地获取信息,这就促使了无线网络从无线互联网络(Wireless Internet)向无线移动互联网络(Wireless Mobile Internet,WMI)[1]的演化,毫无疑问,对于移动用户和网络运营商来说,通过认证密钥协商协议来确认网络和用户的身份,已成为这种环境中的一个基本安全问题。

对许多移动互联网络的用户而言,在享受移动互联网络服务提供商提供的服务时,他们希望能够保留自己的隐私;而对服务提供商来说,他们希望将服务提供给拥有证书的用户或者是完全信任的用户。显然,匿名的服务无法保证服务提供商的信任要求,而提供证书的服务则会透露用户信息。因此,需要一种新的无线匿名服务,以满足以上的安全需求。

移动互联网络双向认证和密钥协商协议,除了具有有线双向认证和密钥协商协议的安全需求之外,还提出了特殊的安全需求[2,3]:

(1)双向身份认证:指移动用户与网络之间相互认证身份,这是安全通信中最基本的安全需求。

(2)密钥协商和双向密钥控制:指用户与访问网络之间通过安全参数协商确定会话密钥,不能单独由一方确定,保证一次一密。 这一方面是为了防止由于一个旧的会话密钥泄漏而导致的重传攻击;另一方面也是为了防止由通信中的一方指定一特定会话密钥带来的安全隐患。

(3)双向密钥确认:移动用户与移动网络系统要进行相互确认,确保对方和自己拥有相同的会话密钥。

(4)相关敏感数据的机密性:这特别适用于用户的身份信息, 因为有些用户为了防止自己的所在位置信息和行踪泄漏,需要对自己的身份信息进行保护,即身份信息不能以明文形式在网络传输。

现有的认证协议[4-7]是从无线网络的角度考虑,文献[4,5]提出一个双向的匿名认证协议,这两个协议使用假名实现用户的匿名,这样外部代理需向家乡代理验证用户身份,实现对外部代理的匿名;文献[6]提出一个每次更换密钥的无线匿名认证协议,避免长期使用一个密钥带来的风险;文献[7]使用证书来实现无线用户的匿名性,仍然需要到家乡代理验证用户证书是否合法,而且用户和外部代理没有协商共享密钥,这样就增加以

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60503008);陕西师范大学创新基金(No.2007CXS025)。
作者简介:张婕(1981-),女,硕士研究生,研究兴趣为网络安全;吴振强(1968-),男,副教授,博士研究生,研究方向为匿名通信技术、自适应安全;霍成义(1972-),男,硕士研究生,研究兴趣为网络安全;见晓春(1983-),女,硕士研究生,研究兴趣为网络安全。
收稿日期:2007-08-15 **修回日期**:2007-11-26

后通信的运算量;目前没有针对移动互联网络这种节点和访问接入点都在移动的匿名认证协议。本文主要针对移动互联网络的这种特殊要求,结合 ID 盲公钥[8-10]设计思想,设计出双向的匿名认证和密钥协商协议。该协议满足了用户的匿名要求。

2　基于身份的密码体制简介

Shamir 提出了基于身份的密码体制[11](ID-based Public Key Cryptography,IDPKC),使用用户的名称、Email 地址等任意的字符串计算公钥,委托密钥中心产生该 ID 所对应的私钥。IDPKC 的优点在于可以避免传统的基于证书的 PKI 系统中使用证书带来的维护成本高,证书链处理过于繁琐等弊端。Shamir 在 1984 年提出 IDPKC 的思想的同时,就给出了令人满意的基于身份的数字签名方案和身份识别方案,但是 Shamir 没有找到他满意的如何设计基于身份的加密系统的方法。我国的陶仁骥教授利用有限自动机提出了一个基于身份的加密系统[12]。国外在 1986 年~2000 年期间提出的几个基于身份的加密系统要么计算太复杂,要么需要防篡改的硬件支持,要么需要防止用户合谋,因此并不实用。2001 年,Boneh 和 Franklin 提出了一个实用的基于身份的加密方案[13](Identity-Based Encryption,IBE),该系统使用了椭圆曲线的 Weil 对,可以证明,该系统能够抵抗选择密文攻击(CCA)。这个方案提出不久后发现,该系统还能扩展为新的密码系统,具有提供认证、抗抵赖以及支持分层构造等多种功能。目前基于身份的密码学已经成为密码学界的一个研究热点。

双线性映射[13]是基于身份的密码体制中非常重要的概念,双线性映射可以从椭圆曲线中的 Weil Pairing 或 Tate Pairing 构造得到。

设 G_1 是一个阶为 q,生成元为 P 的加法循环群,设 G_2 是阶为 q 的乘法循环群,其中 q 是一个大素数。如果满足以下三个条件:

(1)双线性:$\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\cdot\hat{e}(P_2,Q)$,$\hat{e}(P,Q_1+Q_2)=\hat{e}(P,Q_1)\cdot\hat{e}(P,Q_2)$,$\hat{e}(aP,bP)=\hat{e}(P,Q)^{ab}$。

(2)非退化性:如果 P 是 G_1 的生成元,那么 $\hat{e}(P,P)$ 是 G_2 的生成元,即 $\hat{e}(P,P)\neq 1$。

(3)可计算性:$\hat{e}(P,Q)$ 可有效地计算。

则映射 $\hat{e}:G_1\times G_1\rightarrow G_2$ 称为双线性映射。

3　移动互联网络的匿名认证协议

一个移动互联网络主要由四部分构成,如图 1 所示。移动节点(Mobile Node,MN)、移动接入点(Mobile Access Point,MAP)、外部代理(Foreign Agent,FA)和家乡代理(Home Agent,HA)。MH 和 MAP,MAP 和 FA 之间通过无线信道进行通讯,而 FA 和 HA 之间通过有线网络连接。其中 MAP 具有一定的计算能力。由于无线网络和移动互联网络的结构不同,所以无法照搬原有的匿名认证协议,本文把移动互联网络的匿名认证协议分为两个部分:

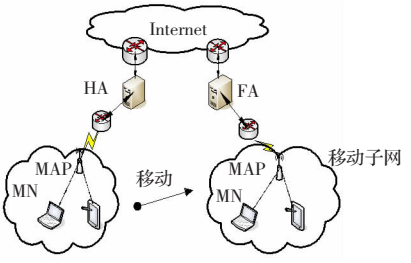

图 1　移动互联网络结构图

(1)第一部分是 MN 对 MAP 的相互认证;

(2)第二部分是 MAP 对 HA 的身份认证。

3.1　基本标识符

首先介绍采用的描述协议的标识符:

$A\rightarrow B:X$:A 向 B 发送消息 X;

PID_A:实体 A 的临时身份标识符;

$\{X\}_K$:用对称密钥 K 对消息 X 进行加密得到的密文;

$E_K(X)$用密钥 K 对消息 X 进行非对称加密;

K_{AB}:在 A、B 之间共享的对称密钥;

PK_A,SK_A:A 的公钥/私钥对;

MN,MAP,HA,FA:移动用户的真实身份标识、移动访问控制点、外部代理和家乡代理;

T_A:由 A 产生的时间戳;

H_1,H_2,H_3:三个不同的 HASH 函数。

3.2　认证过程

3.2.1　MN 对 MAP 的相互认证

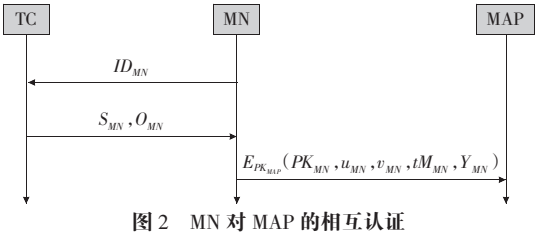

图 2　MN 对 MAP 的相互认证

基于身份公钥的认证方案,在移动子网内部由 MAP 验证用户身份,该方案包含 3 方:可信中心(TC)、移动用户(MN)和验证者(MAP)。认证分为 3 个阶段:系统初始化、用户注册与验证身份。设 G_1 与 G_2 分别是阶为 q 的加法群和乘法群,其中 q 是素数,在 G_1,G_2 中离散对数问题都是难解的。设 $\hat{e}$ 是 $G_1\times G_2$ 到 G_2 的一个双线性映射。通常 G_1 为有限域 Fq 上的椭圆曲线有理点群的一个加法子群,G_2 为这个有限域的一个乘法子群,双线性映射 $\hat{e}$ 由椭圆曲线上的 Weil 对派生得到。设 ID 是个标识用户身份的一个字符串,H 是公开的哈希函数,$H_1,H_2:\{0,1\}^*\rightarrow G_1$。

(1)系统初始化:可信中心 TC 随机选择 $P\in G_1,s\in F_q$,计算 $P_{TC}=sP$。公开 P 和 P_{TC},秘密保存 s。P_{TC} 为系统公钥,s 为系统私钥(亦称系统主密钥),系统中所有用户的私钥均由它生成。

(2)用户注册:假设用户 MN 身份信息为 ID_{MN},计算 $Q_{MN}=H_1(ID_{MN})$,$O_{MN}=H_2(ID_{MN})$,然后将 ID_{MN} 送给 TC。

①TC 计算 $Q_{MN}=H_1(ID_{MN})$,$O_{MN}=H_2(ID_{MN})$,用作日后确认 MN 的身份。然后计算 sQ_{MN} 和 $M_{MN}=s(sQ_{MN}+sO_{MN})$,将 sQ_{MN},sO_{MN} 和 M_{MN} 通过安全信道送给 MN;

②MN 的私钥为 $SK_{MN}=sQ_{MN}$,MN 秘密保存 M_{MN} 和 sO_{MN}。显然 M_{MN} 只能从 TC 得到,无法自己生成。

(3)一次性公钥　任意选择 $t\in F_q$,计算 $PK_{MN}=tQ_{MN}$,$u_{MN}=t(sQ_{MN})$,$v_{MN}=t(sO_{MN})$,则 $(PK_{MN},u_{MN},v_{MN},tM_{MN})$ 称为 MN 的一次性公钥。如果 MN 要与 MAP 进行通信,需要将该一次性公钥和生成的会话密钥生成信息用 MAP 的公钥加密后送给 MAP。MAP 解密后首先验证一次性公钥的有效性,然后通过与之对应的方案对 MN 进行身份认证并保存会话密钥生成信息作为协商密钥的一部分。对一次性公钥的有效性验证描述如下:

①MAP 验证等式 $\hat{e}(u_{MN},P)=\hat{e}(PK_{MN},P_{TC})$ 是否成立。如成立,

则证明 MN 已在 TC 注册过。事实上,$\hat{e}(u_{MN},P)=\hat{e}(t(sQ_{MN}),P)=\hat{e}(tQ_{MN},sP)=\hat{e}(PK_{MN},P_{TC})$。

如果上式成立,则说明 u_{MN} 含有系统主密钥,因此 MN 在 TC 注册过。

②MAP 验证等式 $\hat{e}(tM_{MN},P)=\hat{e}(u_{MN},P_{TC})\cdot\hat{e}(v_{MN},P_{TC})$ 是否成立。如成立,则确信 TC 在必要时可以揭示出 MN 的身份。

事实上,$\hat{e}(tM_{MN},P)=\hat{e}(tssQ_{MN}+tssO_{MN},P)=\hat{e}(tssQ_{MN},P)\hat{e}(tssO_{MN},P)=\hat{e}(tsQ_{MN},sP)\hat{e}(tsO_{MN},sP)=\hat{e}(v_{MN},P_{TC})\hat{e}(u_{MN},P_{TC})$。

如果上式成立,则说明 $tM_{MN}=su_{MN}+sv_{MN}$。而 u_{MN},v_{MN} 也都含有系统主密钥,因此用户 MN 自己无法独立生成 su_{MN},sv_{MN},因而也就无法独立生成 tM_{MN},只能通过从 TC 得到的 M_{MN} 与某个随机数相乘来生成。于 $M_{MN}=s(sQ_{MN}+sO_{MN})$ 且用户 MN 无法伪造,而 TC 中保存了与 MN 相关的 Q_{Mn} 和 O_{MN} 等信息,所以 MAP可以确信 TC 在必要时通过 u_{MN},v_{MN} 能够揭示出用户 MN 的身份。

3.2.2　MAP 对家乡代理的身份认证

当移动子网移动到外地网络进行访问时,外地网络的代理 FA 首先要对其进行认证。为了在协议中实现对移动用户身份的保密性,防止窃听者对其进行跟踪,MAP 不能向 FA 出示其身份标识。因此 FA 对 MAP 的认证是通过 FA 对 HA 的认证与 HA 对 MAP 的认证来实现。在 MN 对 FA 的访问过程中,我们通过 MAP 向 FA 出示只能够由 HA 验证其真实身份的信息来实现用户匿名。

(1)当移动子网进入一个新的网络 FA 时,发送访问请求,开始 MAP 与 FA 的相互认证过程。MAP 计算自己的假名 $PID_{MAP},E_{PK_{HA}}(Y_{MN}//PK_{MN})$ 和及其家乡代理的标识 ID_{HA} 一同发送给 FA。其中,Y_{MN} 是 MN 生成的会话密钥生成信息,$PID_{MAP}=H_3(ID_{MAP})\oplus ID_{MAP}\oplus ID_{HA}$,"⊕"表示按比特的异或运算,"||"为连接符。

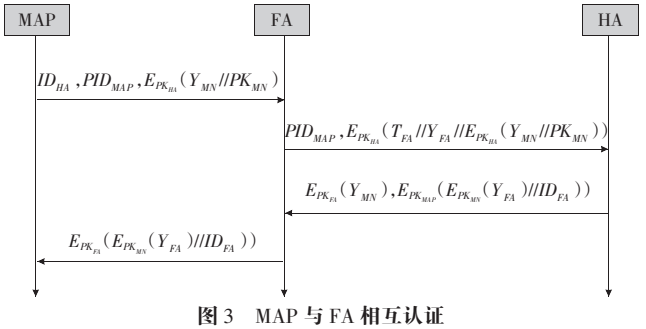

图 3　MAP 与 FA 相互认证

(2)FA 收到 MAP 的访问请求后,转发 PID_{MAP} 并用 HA 公钥加密 $T_{FA}//E_{PK_{HA}}(Y_{MN}//PK_{MN})$ 给 HA 验证身份,其中 T_{FA} 是 FA 产生的时戳。

(3)收到 FA 发送的信息后,首先 HA 用自己的私钥解密,然后 HA 检查时戳是否在有效期,假如时戳失效,HA 拒绝认证 MAP 身份,否则,HA 计算 MAP 的真实身份

$ID_{MAP}=PID_{MAP}\oplus H_3(ID_{HA})\oplus ID_{HA}$。

(4)收到 HA 发送的信息,FA 解密后得到 MN 会话密钥生成信息,FA 将做以下工作:①计算协商密钥;②给 MAP 发送信息 $E_{MAP}(PK_{MN}(Y_{FA})//ID_{FA})$。

(5)MAP 解密信息,把 $PK_{MN}(Y_{FA})$ 转发给 MN,MN 计算会话协商密钥,完成密钥协商。

这里使用基于 ECC 的 Diffie – Hellman 算法来计算协商密钥,协议原理如下:

首先:MN 选择一个随机大整数 x,并向 FA 发送 $Y_{MN}=xP$;

其次:FA 选择一个随机大整数 y,并向 MN 发送 $Y_{FA}=yP$;

最后:MN 和 MAP 分别计算会话密钥 $K=yY_{MN}=xY_{FA}$。

3.2.3　一次一密

在这个协议中,每次会话都会改变密钥,这样移动用户 MN 可以经常更改密钥,减少长期使用一个密钥带来的风险。

(1)$MN\rightarrow MAP:(Y_{MN,i}//K_{i-1})_{K_{i-1}}$

(2)$MAP\rightarrow FA:ID_{FA},PID_{MAP},(Y_{MN,i}//K_{i-1})_{K_{i-1}}$

(3)$FA\rightarrow MN:(Y_{FA,i})_{K_{i-1}}$

假如 MN 需要第 i 次更新会话密钥,MN 可以根据上式获得新的密钥。新的会话密钥 K_i 计算如下:

$K_i=y_iY_{MN,i}=x_iY_{FA,i},i=1,2,3,\cdots,n$。

K_0 是首次密钥协商出的共享密钥。

4　协议的性能分析

4.1　用户与服务器之间密钥的安全性、新鲜性和公正性

MN 在计算出 K 后,FA 使用相同的方法产生会话密钥,由于每次通信前选择了不同的随机数 x、y 计算会话密钥,MN 与 FA 每次通信均采用不同的会话密钥,从而确保了密钥的新鲜性,有效地防止了重放攻击。会话密钥由 x 和 y 共同决定,任何一方都不能单独产生会话密钥,保证了密钥的公正性。因此任何第三方都无法利用先前截获的消息发起重放攻击。

4.2　移动用户身份的匿名性和不可否认性

用户 MN 的一次性公钥为 $(PK_{MN},u_{MN},v_{MN},tM_{MN})$,它们都经过了随机数 t 的处理,因此没有向 MAP 泄漏任何有关 MN 的私钥信息。并且,在上述 MN 向 MAP 证明自己身份的过程中,MAP 仅能知道 MN 已在可信中心 TC 注册过,并确信 TC 可以揭示 MN 的真实身份。只要 MN 不取相同的 t,每次的公钥就不会相同。因此,MAP 自己无法得知 MN 的真实身份。并且用户 MN 的不同活动之间也没有任何联系,在必要时,MAP 可以与可信中心 TC 合作,来揭示用户 MN 某次活动的真实身份。MAP 只需将 u_{MN},v_{MN} 送给 TC,由 TC 来揭示 MN 的身份。因此,这既保证了用户的活动具有匿名性和不可追踪性,也保证了用户不能进行恶意的活动。在移动子网内部,由于使用一次公钥,攻击者无法将来自同一用户的消息关联起来,从而阻止其跟踪该用户的行踪,称为不可跟踪性。在该协议中,用户对于攻击者并没有提供任何可供关联的信息,因此攻击者无法关联同一次协议执行过程中的消息;同样,攻击者更无法关联不同协议执行过程中的消息,从而有效地保护了用户的身份。在移动子网外部,MAP 使用了假名隐藏自己的身份,攻击者也无法得知 MAP 真实身份。

用户 MN 不能使用虚假的公钥信息对 MAP 进行欺骗。首先,用户无法伪造 sM_{MN}。因为 MAP 通过验证等式 $\hat{e}(u_{MN},P)=\hat{e}(PK_{MN},P_{TC})$ 可以得知 u_{MN} 含有系统主密钥。通过验证等式 $\hat{e}(tM_{MN},P)=\hat{e}(u_{MN},P_{TC})\hat{e}(v_{MN},P_{TC})$,可以得知 $tM_{MN}=su_{MN}+sv_{MN}$。因为 u_{MN},v_{MN} 也都含有系统主密钥,用户 MN 自己无法独立生成 su_{MN},sv_{MN},因而也就无法独立生成 tM_{MN},只能通过从 TC 得到的 M_{MN} 与某个随机数相乘来生成。由于 MN 无法伪造 M_{MN},所以 tM_{MN} 具有不可伪造性。如果 MN 伪造了 u_{MN} 或 v_{MN},MAP 也可以

通过验证等式$\hat{e}(tM_{MN},P)=(u_{MN},P_{TC})\hat{e}(v_{MN},P_{TC})$是否成立来发现。

4.3 双向认证

双向认证的目的是为了保证协议所涉及的通信实体是合法的。通过服务器对用户的认证,防止攻击者假冒合法用户占用网络资源;通过用户对网络的认证,防止假冒服务器的攻击。在会话密钥建立过程中,MN 和 MAP、MAP 和 FA、FA 和 HA 之间都对彼此之间的身份进行验证。在移动子网内,MAP 通过用户的一次性公钥来验证用户的身份, 而用户用 MAP 的公钥加密信息,只有 MAP 才拥有自己的私钥,所以只有 MAP 才能解开密文,得到信息,实现对 MAP 的身份认证。MAP 对家乡代理的身份认证中,MAP 和 FA、FA 和 HA 都用对方的公钥加密信息,这样,也就实现了相互之间的双向身份认证。攻击者若要假冒外地服务器, 由于他没有信任的第三方颁发私钥 SK_{FA} 而无法解密报文,也就无法冒充 FA 和 MN 协商共享密钥,所以这种攻击也是不可能的。

4.4 安全性分析

文中所提协议的计算安全性基于椭圆曲线上离散对数难题和安全单向函数。下面将就一些公钥密码协议常见安全问题进行讨论。

已知密钥安全: 在这个协议中,MN 和 FA 采用基于 ECC 的 Diffie-Hellman 算法来计算协商密钥,而且每次会话都改变密钥,假设攻击者已知一些旧的会话密钥,这对攻击者获取新的会话密钥或者假冒任一参与方都是没有帮助的。

前向安全:假设攻击者得到了 MN 或 FA 的私钥(甚至同时得到 MA 和 FA 的私钥),攻击者也难于获取 MN 和 FA 之间协商的旧会话密钥。因为会话密钥 $K=xY_{FA}=yY_{MN}$ 的 x 和 y 分别是 MN 和 FA 生成的随机数, 它们并不直接在网络中传输,传输的是 Y_{FA} 和 Y_{MN}。由椭圆曲线上离散对数难题知,A 攻击者很难由 Y_{FA} 和 Y_{MN} 反推出 x 和 y,所以也就无法知道会话密钥,协议向前安全。

重放攻击:假设攻击者重放 MN 的消息,由于用户的公钥是一次性的,MAP 可以查看用户的公钥是否相同轻易的挫败对该消息的重放,攻击者除了通过重放来延迟或破坏协议的执行外,不会构成实质威胁。并且为了保证会话密钥的新鲜性,每次执行认证协议,认证双方都要随机选择数 x 和 y,只要认证双方有一方是合法的并按协议的规则执行,则攻击者重放已经截获的信息无法得到有效的会话密钥,同时其身份认证也无法通过。

中间人攻击:在传统的 Diffie-Hellman 协议中,攻击者能用自己的值替换来自 A 的公钥($g^a \bmod n$)或 B 的公钥($g^b \bmod n$),从而与 A 和 B 分别共享不同的密钥,而不被 A 和 B 发现攻击者。在本协议中,由于用户使用一次性公钥,假如攻击者冒充 MN 给 MAP 发送信息,MAP 很容易就验证出用户是否在 TC 中注册过, 所以攻击者无法冒充 MN; 攻击者也无法冒充 FA 与 MN 协商密钥,因为在协议第二部分的 HA 向 FA 发送信息中,FA 才能知道 MN 的协商密钥信息,而这一部分信息 HA 用 FA 的公钥加密,只有 FA 才拥有自己的私钥,得到 MN 的协商密钥信息,攻击者无法知道该密钥信息,因此无法和 MN 建立共享密钥 K,同样 FA 也不能和攻击者建立共享密钥 K,因此协议能防止中间人攻击。

4.5 协议效率

考虑到移动端和网络端计算能力的差异,在这里主要考虑移动用户的运算量。

(1)计算量:移动端需要进行两次公钥加/解密运算和 1 次哈希函数运算;

(2)交互次数:移动端需要与移动访问接入点进行两次交互。

协议与其它协议比较结果如表 1 所示。

表 1 协议计算开销比较表

协议	文献[4]	文献[6]	文献[7]	新协议
散列运算次数	4	2	1	1
对称加密/解密	2	3	1	0
公钥加密/解密	1	0	2	2
模指数运算次数	5	0	4	2
用户交换信息次数	3	3	5	2
提前密钥协商	N	Y	N	N
双向认证	Y	Y	N	Y
协商密钥	Y	Y	N	Y

从表 1 可以看出,与其他协议相比,新协议的用户只进行了 1 次 hash 运算,2 次模指数运算,2 次公钥加解密运。不难看出,新协议的计算开销较文献[3]和文献[7]的计算开销要小。因为文献[6]中用户提前与家乡域协商过密钥,所以运算开销比其他协议小。新协议用户不需要到家乡代理去验证身份,通过椭圆曲线 Weil 对的双线性特征验证用户的身份真实性, 使该协议在更小密钥量下提供了更大的安全性, 所需带宽明显减少,而且提供更的匿名度,减少运算开销。与其他协议相比,新协议更高效、更实用。

5 结束语

作为移动互连网络的一种解决方案,匿名认证协议及其安全性越来越引起研究人员的重视。本文利用基于身份的公钥系统, 提出一个移动互联网络的双向匿名认证和密钥协商方案,解决了移动用户和移动互联网络之间的双向身份认证和密钥协商问题,并使移动网络系统向移动用户提供匿名服务,使访问网络和非法窃听者都不能获得用户的真实身份信息,最大程度保证了用户身份信息和所在位置信息的机密性,整个协议实现简单、高效实用,是解决移动互联网络安全问题一个可行的方案,同时对于使用基于身份公钥来解决移动通信中的身份认证和密钥协商问题也有一定的借鉴意义。

参考文献:

[1] 吴振强,马建峰.基于管理的移动互联网络安全体系结构[J].计算机科学,2006,33(7)专刊.

[2] Horn G,Preneel B.Authentication and payment in future mobile systems[C]//Computer Security ESORICS'98 Proceedings.Berlin:Springer Verlag,1998:277-293.

[3] Horn G,Martin K,Mitchel C J.Authentication protocols for mobile network environment value-added services[J].IEEE Transactions on Vehicular Technology,2002,51(2):383-392.

[4] 邓所云,胡正名,钮心忻,等.一个无线双向认证和密钥协商协议[J].电子学报,2003,31:135-139.

[5] 万仁福,李方伟,朱江.匿名双向认证与密钥协商新协议[J].电子科技大学学报,2005,34(1):61-64.

[6] JIANG Yixin,LIN Chuang.Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks[J].IEEE Transations on Wireless Communications,2006,5(9):1-8.

(下转 109 页)