移动计算网络环境中的认证与小额支付协议

姬东耀, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 本文在分析现有移动用户认证协议与因特网认证协议基础上, 针对移动计算网络的技术特点设计了一个用于移动用户与收费信息服务网络相互认证和用户进行小额电子支付的协议, 该协议的新颖之处在于把小额支付方案融入认证协议当中, 使移动用户可以利用笔记本电脑或掌上电脑进行付费的网面浏览、购买低价位信息商品以及进行移动电子商务, 同时也为移动用户漫游时的记费提供了依据. 协议不仅在公共参数的存储空间需求和用户端计算负荷上是适当的, 而且可以保护用户不被错误收费, 同时提供服务网络防止用户抵赖的合法证据. 该协议基于一个全局的公钥基础设施, 适用于未来的基于第三代移动通信系统的网络计算环境.

关键词: 移动计算网络; 认证; 小额电子支付; 公钥基础设施.
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2002) 04-0495-04

An Authentication and Micropayment Protocol for Mobile Computing Network

JI Dong-yao, WANG Yu-min
(*National Key Lab on ISN, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: According to the requirements of the technique in mobile computing network, an efficient protocol for mutual authentication and electronic payment for mobile computing network is proposed. The paper also demonstrates how a micropayment scheme can be integrated into the authentication protocol. The protocols provide security services required by regular authentication and payment protocols and are efficient in consideration of the storage requirement and computation overheads on subscribers. They protect subscribers from incorrect service charges and provide service providers legal evidences to collect bills that are denied. By using public key infrastructure, they can be used as authentication and payment protocol in future mobile systems.

Key words: mobile computing network; authentication; micropayment; public key infrastructure

1 引言

移动计算网络是用户计算机可以在网内随意移动的计算机通信网络, 用户可以在无线网络覆盖的任何地方随时发送和接收各种数据信息, 而且可以在不同地区(甚至不同国家)之间进行漫游. 与一般的有线网络相比, 移动网络的安全性要求更高, 主要表现在: 无线电波自由传播, 易被窃听, 需要更复杂的加密技术; 用户移动范围广, 必须有一网管中心负责用户移动性管理、网络安全管理、数据库管理, 包括用户注册和认证、计费、用户位置登记、用户漫游管理、越区切换等; 用户终端有一定的计算能力和存储能力, 它可能通过有线或无线方式接入因特网进行网页浏览、电子邮件收发、利用文件传输协议进行文件传输、加入新闻讨论组、接收多媒体视频服务以及进行电子支付和电子签定合同等因特网业务[1]. 如果这些业务不是免费的, 那么还有一个小额电子支付问题. 而用户和服务网络之间信息服务与付款信息的公平交换要具有非否认功能必须采用数字签名, 这就需要一个全局的公钥基础设施. 针对这些问题, 本文设计了一个适用于移动计算网络环境的移动用户认证与支付协议, 并对这一协议性能进行了分析.

2 原有协议的分析

迄今, 人们针对移动通信系统以及个人通信系统设计了许多认证与会话钥建立协议[2-5], 这些协议主要采用对称钥加密算法和杂凑算法, 利用随机数挑战进行认证. 若把这类协议直接用于移动计算网络环境中有一定的局限性, 这主要表现在移动计算环境中的用户终端有一定的计算与存储能力, 它可以接入因特网进行诸如网页浏览、电子商务、视频点播等业务, 而不只局限于话音业务. 同时对于一个全球移动计算网络来说, 要进行可靠的认证与支付, 需要利用公钥基础设施. 为了克服这些缺陷, 有关学者针对第三代移动通信系统提出了一个认证与会话钥建立协议[6], 这一协议虽然利用了公钥

收稿日期: 2000-09-11; 修回日期: 2001-04-13
基金项目: 国家自然科学基金(No. 19931010); 高等学校博士点基金(No. 2000070101)

基础设施,但没有提供前向安全[7]功能,一旦服务提供者的私钥泄露,就可能造成非法服务提供者对用户的欺骗.而且这一协议不能保护用户的匿名性,用户和服务提供者相互认证时需要验证一个很长的证书链.这些缺陷是进行移动电子商务所不能允许的.为此我们设计了一个移动计算环境的认证与支付协议.我们的协议设计既体现了移动通信协议尽可能采用杂凑运算和对称加密以减少认证时延的特点,又体现了因特网协议多采用公钥加密以利于密钥分配的特点[8],同时把小额支付协议[9]融入认证与会话密钥建立协议.新协议具有完善的前向安全特性和用户匿名性,而且借助于用户的网管中心简化了证书验证过程.从而可使移动用户利用手持电脑进行移动电子商务,同时也为移动用户漫游时的记费提供了依据.

3 移动计算环境的认证与支付模型

移动计算环境中的认证与支付主要涉及三方:用户 U,提供信息服务的网络 SN,用户 U 和 SN 信任的第三方 TTP(通常为用户的网管中心).用户 U 和信息服务网络 SN 在 TTP 处都维持一帐户,这一帐户和常规的银行帐户相联系.这里服务网络 SN 可能是本地 IP 子网也可能是外地 IP 子网,因此 SN 和 U 的公钥证书可能是由不同证书管理机构(CA)颁发的,但这些 CA 在认证方面都属于一全局的公钥基础设施,各 CA 由一全局 CA 分级管理,用户和服务网络之间可以通过证书链方式得到对方公钥,我们使用时把它看作一个整体.用户帐户可以从银行补充资金,同时 SN 的帐户里的资金可以存入银行.

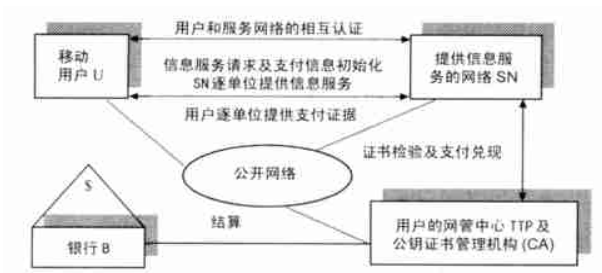

图 1 移动计算环境的认证与支付模型

当移动用户 U 想从信息服务网络 SN 中得到信息服务时,他首先和 SN 执行一认证与会话钥建立协议,并在认证与会话钥建立过程中进行支付的初始化.服务提供者 SN 在网上公布信息服务目录,其中包括每项服务的计费单位 L(如视频服务的 1 分钟、5 分钟或电子出版物的一页)和价格 P 以及每项服务包含的计费单位数 m.用户通过移动终端的浏览器选择服务项目,然后执行服务请求协议,通过协议的执行用户向服务提供者作支付承诺,服务提供者给用户解密加密信息的密钥,其后用户根据他得到的服务单位数不断向 SN 提供能使 SN 能够进行公平记帐的证据,SN 最后能利用这些证据与 TTP 兑现这些支付,同时网管中心也收取一定的管理费用.系统模型如图 1 所示.

4 移动计算环境的认证与支付协议

4.1 认证与支付初始化协议 P1

下面的协议描述中,idS 用来标识信息服务网络 SN,协议开始执行时移动用户 U 知道这一标识 idS.服务网络 SN 的私钥为 v,公钥为 g^v,SN 的公钥证书为 $certS$;g 为 $GF(P)$ 上的本原元,P 为大素数,P,g 由系统的公正机构选择.用户 U 的身份为 idU,公钥为 g^U,公钥证书为 $certU$;用户网管中心标识为 $idTTP_U$,$idTTP_U$ 的公钥为 g^w.$\{M\}_K$ 表示消息 M 用密钥 K 进行对称加密的结果;$Sig_U(M)$ 表示用户 U 对消息 M 的数字签名;h、h_0、h_1、h_2 和 h_3 是抗碰撞单向杂凑函数;$\|$ 表示消息级联.服务请求与支付初始化协议如图 2.

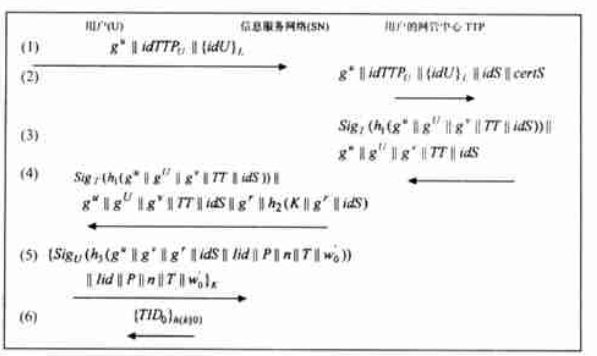

图 2 TTP 参与下的认证与会话密钥建立及服务请求与支付初始化协议

下面对协议进行详细描述:

当用户 U 想从一信息服务网络 SN 中得到信息服务时,他和 SN 先执行认证与会话密钥建立协议.协议的执行过程如下:

(1) U 产生一随机数 u 并计算 g^u,并把 g^u,U 的 TTP 的标识 $idTTP_U$ 及加密的用户身份发送给 SN.其中,$L = g^{uw}$,L 为 U 与 $idTTP_U$ 共享密钥,g^w 为 $idTTP_U$ 的公钥.

(2)SN 收到消息(1)后,若用户的 TTP 也是它所信任的,则把这一消息附加上自己的身份及证书 $certS$ 转发给 TTP.

(3)TTP 用它和用户的共享密钥 L 解密 $\{idU\}_L$ 得到用户身份,在数据库中搜索一条 CA 最新公布的证书吊销列表 CRL,检查证书是否被吊销,同样对于 SN 的证书也要检查.若证书合格,则 TTP 对提取的系统时间 TT、U 的公钥 g^U、SN 的公钥 g^v、消息摘要 $h_1(g^u \| g^U \| g^v \| TT \| idS)$ 签名并发给 SN.

(4)收到消息(3)后,SN 验证 TTP 的签名对 TTP 进行认证,从而确认了 U 的公钥 g^U 没有吊销,他存储消息(3)然后转发给 U,另外 SN 产生一随机数 r,并计算 g^r、$(g^u)^r$、$(g^u)^v$,产生一它和用户共享的会话钥 $K = h_0((g^u)^v \| (g^u)^r)$.它计算 $h_2(K \| g^r \| idS)$,并把它和 g^r 一同发给 U.

(5)收到消息(4)后,U 通过对 TTP 签名的验证确认了 SN 的公钥没有吊销,它计算 $K = h_0((g^u)^v \| (g^u)^r)$,进而通过对 $h^2(K \| g^r \| idS)$ 的验证认证了 SN,并确定 SN 知道会话密钥 K.U 选取随机数 w_n',生成一条杂凑链 w_0',w_1,w_1',w_2,w_2',…,w_n,w_n',其中 $w_i = h(w_i')$,$w_{i-1}' = h(w_i)$,$i = n, n-1, \cdots, 1$.w_0' 叫做杂凑链的根,用户可以利用它向服务提供者承诺.U 然后计算 $g^u \| g^v \| g^r \| idS \| Iid \| P \| n \| T \| w_0'$ 的杂凑值,再对这一杂凑值及 $Iid \| P \| n \| T \| w_0'$ 签名,并把这一消

息用它们的共享会话密钥 k 加密后发送给 SN. Iid 是请求服务标识; P 为服务价格; n 是请求的信息服务单位数; T 是请求时间.

(6) 收到消息(5) 后, SN 利用它与用户 U 的共享密钥 k 解密这一消息, 然后用 U 的公钥验证 U 的签名, 并检查消息摘要, 从而获得对 U 的认证. SN 为 U 产生一临时身份 TID_0, 并用共享密钥 $h(k \| 0)$ 加密发给 U, U 后续连接中就可用此身份, 从而实现 U 对 SN 的匿名访问. 同时 U 对 w'_0 的签名使用户 U 对其后提供的杂凑值不可否认. U 对 Iid, p, n, T 的签名是用户进行服务请求的不可否认证据, 也为 SN 收费提供了依据.

4.2 信息服务与支付协议-P2

用户 U 和访问网络执行了认证及支付初始化协议后, SN 把服务信息分成 n 个单位, 开始逐单位为 U 提供服务, 用户 U 把 (w_i, w'_i) 组成一对, 作为他对一个单位服务的支付, 每次用户 U 首先向 SN 发送前一半 w_i, SN 检查是否有 $w'_{i-1} = h(w_i)$, 若不相等, 则不提供第 i 个单位服务; 若相等, 则提供第 i 个单位服务. 当 U 得到第 i 个单位服务时, 再提供另一半 w'_i. 若 U 提供了前一半 w_i, 但 SN 没有提供第 i 个单位服务; 或者 U 得到了第 i 个单位服务, 但没有提供另一半 w'_i, TTP 同样按照 U 得到 i 个单位服务记费, 而 SN 也只能得到 $i-1$ 个单位服务的费用, 第 i 个单位服务的费用充公用于公益事业. 这样 SN 和 U 无论谁中断都得不到好处. 并且协议也不会带来通信负荷的增加, 因为 w'_i 可以和 w_{i+1} 合在一起发送. 进一步因为 w'_i 可以从 w_{i+1} 计算出来, 所以可以只发 w_{i+1}. $h(k \| 0)$ 用作信息加密钥. TID_i 为 SN 给 U 分配的后续第 i 次服务的临时身份, 第 i 次服务信息加密钥为 $h(k \| i)$.

$U \xrightarrow{} SN$: $TID_0, w_1, 1$　　$SN \xrightarrow{} U$: 第一个信息服务单位

$U \xrightarrow{} SN$: $w_2, 3$　　$SN \xrightarrow{} U$: 第二个信息服务单位

⋮　　⋮

$U \xrightarrow{} SN$: $w_n, 2n-1$　　$SN \xrightarrow{} U$: 最后一个服务单位

$U \xrightarrow{} SN$: $w'_n, 2n$　　$SN \xrightarrow{} U$: $\{TID_1\}_{h(k \| 1)}$

在每天(或别的适当日期) 结束时, SN 把他最后收到的每条杂凑链的值及服务请求协议中的消息发给 TTP, TTP 根据最后收到的每条杂凑链的值计算出用户得到多少单位服务(例如 SN 收到的最后一个杂凑值为 w'_c, 由协议 $P1$ 的(5) 及 $h^{2(n-c)}(w'_c) = h^{2n}(w'_n) = w'_0$, 可确定 SN 向 U 提供了 c 个单位服务). 再根据每个单位的价格, TTP 计算出 U 应该给 SN 的支付量, 并从 U 的帐户扣除相应数量和给 SN 的帐户存入相应数量. 而且 TTP 可以非在线的处理这些支付信息, 不会成为瓶颈.

5 新协议的性能分析

(1) 用户的匿名性. 在 $P1$ 协议中, 用户 U 的身份 idU 用 U 与他的 TTP 的共享密钥加密, SN 无法对此解密得到 idU, 只有 TTP 可以将其解密. 而证书的检验是在 TTP 中进行的, SN 只知道检验结果, 并不知道用户身份. 在 $P2$ 协议中, 用户只需向服务网络 SN 提供临时身份 TID, SN 仍然不知道用户的真实身份. 此外, 窃听者也无法从所截获的消息流中获得关于用户身份的信息.

(2) 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, 特别对于第三代通信网这样的异构网络来讲, 双向认证是防止假冒攻击, 保证网络安全运行的重要措施. 下面对 $P1$ 和 $P2$ 协议抗假冒攻击能力进行分析.

攻击者若要假冒用户, 他要么获取合法用户 U 的私有签名钥, 要么重放上次会话中 U 所发送的信息, 获取用户私钥显然是很困难的, 而重放消息则可以通过对服务请求时间 T 和消息摘要 $h_3()$ 检验加以识别.

攻击者若要假冒 SN, 他必须寻找一个有效的信息对 $(r, K) = (r, h_0(g^{uv}) \| (g^u)^r)$, 进而计算 $h_2(K \| g^r \| idS)$, 但这是不可能的, 因为他不知道 u 和 v, 不能导出 g^{uv}; 攻击者也可能在看到一个有效的信息对后直接寻找一个信息对 $(r', h_2(K \| g^{r'} \| idS))$, 可是 U 验证时计算 $K' = h_0(g^{uv} \| g^{uv'})$, 因为 $r \neq r'$, 所以 $K \neq K'$, $h_2(K' \| g^{r'} \| idS) \neq h_2(K \| g^r \| idS)$.

攻击者若要假冒 TTP, 则需要知道 TTP 的签名私钥, 这也是十分困难的.

在协议 $P2$ 中只有用户 U 能正确的依次出示 $w_1, w_2, w_3, \ldots, w_n$ 所以攻击者不能假冒 U.

(3) 业务的不可否认. 首先用户及服务网络公钥证书的在线检验保证了他们公钥的有效性. 其次 U 对 w'_0 的签名为网管中心记费提供了不可否认依据. 若 U 想抵赖, SN 可出示 U 最后发给它的杂凑值, 对此用户无可争辩, 因为只有他能产生这一值, SN 无法伪造. 若 SN 想多收费, 他必须能从 w_i 导出 w_{i+1}, 但由杂凑函数 $h()$ 的单向性, SN 很难导出. 最后 U 对服务名称、价格、时间等的签名使他对所接收服务不可否认. U 对 g^u, g^v, g^r 的签名及协议 $P1$ 中的消息(4) 使得双方对信息加密钥的协商不可否认.

(4) 用户端计算负荷较小. 用户端的计算负荷主要体现在协议 $P1$ 中, 在消息(1) 中他要做一个对称加密运算, 收到消息(4) 后做一次签名验证运算, 在消息(5) 中做一次签名运算. 若采用椭圆曲线数字签名, 采用 160bit 密钥和 MD5 杂凑函数, 对这些消息签名和验证在没有密码协处理器的情况下 1s 内就可完成. 这对于一般掌上电脑是完全可以实现的. 而协议 $P2$ 每次用户只做一次杂凑运算, 用户可以预先计算出要发给 SN 的杂凑值, 在一适当的时间间隔自动释放这些杂凑值.

(5) 支付协议的公平性. 若 SN 得到了前一半杂凑值而不给用户提供服务, 他用这一半杂凑值不能得到支付. 同样, 若用户发了前一半杂凑值, 得到服务后不发后一半杂凑值, 他照样要为这一单位信息商品付费. 所以无论谁先中断协议都得不到好处.

(6) 前向安全功能. 因为用户和信息服务网络协商的会话密钥由他们各自产生的随机数 u 和 r 决定, 所以, 即使其中一方的长期密钥被合谋, 其后会话中使用的会话密钥仍是安全的.

6 结束语

本文设计了一个移动计算环境下的认证与支付协议, 除了用于用户认证与小额支付外, 协议也建立了用户和服务网

络的会话密钥以及加密信息产品的密钥. 协议设计既体现了移动通信协议尽可能采用杂凑运算和对称加密以减少认证时延的特点, 又体现了因特网协议多采用公钥加密以利于密钥分配的特点, 同时融入了小额支付协议, 使它可用于移动电子商务.

参考文献:

[1] Z J Hass, R Alonso, D Duchamp, B Gopinath. Special issue on mobile and wireless computing networks [J]. IEEE Journal on Selected Areas in Communications, 1995, 13(5): 839- 923.

[2] R Molva, D Samfat, G Tsudic. Authentication of mobile users [J]. IEEE Network, 1994, 8(2): 26- 34.

[3] S Mohan, Privacy and authentication protocols for PCS [J]. IEEE personal communications magazine, 1996, 3(5): 34- 38.

[4] L Harn, H Lin. Modifications to enhance the security of GSM [A]. Proc 5th Nat Conf on Information Security[C]. Taiwan, 1995. 97- 100.

[5] Y Frankel, A Herzberg. Security issues in a CDPD wireless network [J]. IEEE Personal communications magazine, 1995, 2(4): 16- 27.

[6] ETSI SMG/SG/TD-73. Protocols for UMTS Providing Mutual Authentication and Key Establishment Using Asymmetric Techniques[S].

[7] M Bellare, S K Miner. A forward - secure digital signature scheme [A]. Proc. Cryto' 99[C]. Berlin: Springer. 1999. 431- 448.

[8] S M Bellovin, M Merrit, Limitation of the kerberos authentication system [J]. Computer Communication Review, 1990, 20(5): 119- 132.

[9] R L Revest, A Shamir. Payword and micromint: two simple micropayment schemes [A]. Proc. Security Protocol[C]. Berlin: Springer, 1997. 69- 87.

作者简介:

姬东耀 男, 1966 年生于陕西榆林, 博士生, 1996 年在西安电子科技大学获硕士学位, 从 1998 年起在西安电子科技大学通信工程学院攻读博士学位, 研究方向为网络安全与保密.

王育民 男, 1936 年生, 教授, 博士导师, 长期从事编码、密码和信息论的教学科研工作.