文章编号: 1001-0920(2004)04-0474-04

GSM 网络环境上椭圆曲线密码系统身份认证协议的研究

周福才, 曹光辉, 黄 宇, 张冠宇
(东北大学 信息科学与工程学院, 辽宁 沈阳 110004)

摘 要: 提出一种将椭圆曲线密码系统身份认证协议应用 GSM 网络上进行身份认证的控制方法. 采用 CA 证书机制, 应用离线获取证书, 在线相互认证提高 GSM 网络系统安全性. 应用无求逆数字签名方案实现 CA 认证, 简化了计算复杂度, 并通过通讯双方数字签名实现不可抵赖性, 最后给出了协议安全分析. 提出的认证协议具有保密性高及传输参数少的优点, 较容易在无线移动通讯系统软硬件中实现

关键词: 椭圆曲线加密系统; CA 证书; 数字签名; 身份认证
中图分类号: TP273 **文献标识码**: A

Identity authentication protocol in GSM network environment based on elliptic curve cryptosystem

ZHOU Fu-cai, CAO Guang-hui, HUANG Yu, ZHANG Guan-yu
(School of Information Science and Engineering, Northeastern University, Shenyang 110004, China. Correspondent: ZHOU Fu-cai, E-mail: fczhou@mail.neu.edu.cn)

Abstract: Identity authentication in GSM network environment is proposed by using identity authentication protocol based on elliptic curve cryptosystem. Applying CA mechanism, obtaining the certification offline, the security of the GSM network system is enhunced by authenticating each other online. The CA mechanism is executed by using the no-inverse digital signature scheme, and the complexity of computing is reduced. The mutual signatures of communication realize the nonrepudiation. The security analysis of the protocol is given. The advantages of this protocol are higher security, less parameters of transmission and easier to realize by the hardware of mobile wireless communication system.

Key words: elliptic curve cryptosystern; certification authentication; digital signature; identity authentication

1 引 言

GSM 是一个被大家广泛使用的无线移动通讯系统, 在这个系统中通常使用 A3, A5, A8 函数来完成用户身份识别与控制以及保障通讯安全[1]. 由于大家对个人隐私的重视以及系统对防止非法使用者的入侵盗打等问题, 使得 GSM 系统的安全性受到质疑, 尤其系统安全依赖于函数 A3, A5 和 A8(算法未公布), 是否安全可靠或藏有暗门就不得而知.

GSM 除了函数本身的安全性问题外, 还有两个主要的安全问题[2, 3]:

1) 拜访位置寄存器(VLR)每次可从归属位置寄存器(HLR)处得到用户信息(R, SRES, K_c), 这样虽然可以加快 VLR 与 HLR 之间的通讯时间, 进而加快速度, 但这些用户信息也很容易被 VLR 中不守法的工作者窃取, 冒充用户的名义来使用, 给用户造成损失.

收稿日期: 2003-02-04; **修回日期**: 2003-09-02
基金项目: 国家自然科学基金资助项目(69874038); 国家高技术研究发展计划资助项目(2001AA115300).
作者简介: 周福才(1964—), 男, 吉林长春人, 副教授, 博士, 从事信息安全、电子商务协议以及认证技术的研究; 曹光辉(1972—), 男, 辽宁锦州人, 讲师, 硕士, 从事网络安全及认证技术的研究

2) GSM 的协议(protocols)中没有直接让用户去识别认证系统身份的功能,所以攻击者可通过重放复制下的随机数 R 来骗取用户的信任,使得用户在不知不觉的情况下,与一个假冒的系统通讯

以椭圆曲线密码理论为基础的公钥密钥系统安全性能佳且效率高,其实现的速度比其他公钥密钥算法(如RSA)更为快捷[6]. 本文将椭圆曲线密码理论应用于 GSM 系统上,设计一套完整认证协议以改善原来 GSM 系统安全上存在的一些问题,该算法省时且易实现

2　GSM 系统的身份认证及其 Lo and Chen 方案

2.1　GSM 认证协议[1,3]

GSM 认证协议如下:

1) 系统设置初始化: GSM 使用A3,A5和A8函数,其算法不对外公开. 其中:A3是一个单向函数,A5是加解密函数,A8是一个生成通信密钥单向函数. 归属位置寄存器(HLR)下的认证中心(AUC)存放移动用户身份标识 MSI 以及使用者的密钥 K_i,移动用户漫游卡上存放身份标识 MSI 及使用者的密钥 K_i.

2) 认证流程: 如图1所示,首先移动用户MS将 MSI 传给VLR,VLR 再将 MSI 传给用户的HLR; 系统产生一个随机数 R,计算 $SERS = A3(E_{K_i}(R))$, $K_c = A8(E_{K_i}(R))$,将 $(R, SERS, K_c)$ 传给VLR;VLR 将随机数 R 传给移动用户MS; 移动用户MS接到 R 计算 $SERS = A3(E_{K_i}(R))$, $K_c = A8(E_{K_i}(R))$; 移动用户MS将 SERS 发给VLR; VLR 收到移动用户发过来的 SERS 与从HLR 得到的 SERS 进行比较,如果相同则为合法用户,就将 ACK 送给移动用户; 如果不同则为非法用户,移动用户与基站之间就可用密钥 K_c 进行通讯

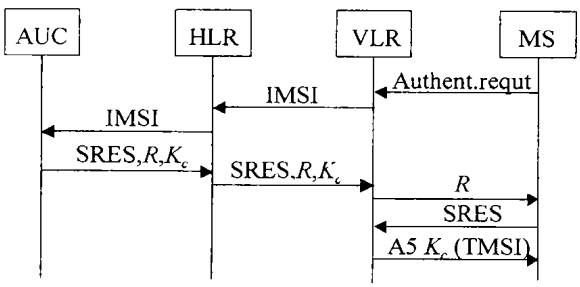

图1　GSM 认证协议流程

2.2　基于 RSA 密码系统的 GSM 身份认证协议

Lo and Chen 提出基于RSA 密码系统来改进现有 GSM 系统认证协议的安全性[1,2],并以公钥密码系统RSA 来识别控制身份,并给出了通信密钥的产生方式

Lo and Chen 提出的 GSM 控制认证协议如下[1,2]:

1) 系统设置初始化: 使用公开密码系统RSA算法; HLR 下的认证中心存放全球移动用户身份标识 MSI 以及对应使用者的公钥($K_{pub,m}$); 移动用户漫游卡上存放 MSI 及私钥($K_{priv,m}$),公钥($K_{pub,m}$).

2) 认证流程: 如图2所示,首先移动用户MS将 MSI 传给VLR,VLR 再将 MSI 传给HLR; 系统产生一个随机数 R 及一个随机数信息 M,将 R 加密计算得到 $E_{K_{pub,m}}(R)$,将 M 加密计算得到 $E_{K_{pub,m}}(M)$,系统再将自己的公钥($K_{pub,s}$)送出. 最后将 $[E_{K_{pub,m}}(R), E_{K_{pub,m}}(M), (K_{pub,s})]$ 由基站(BS)送给移动用户; 移动用户MS 收到 $[E_{K_{pub,m}}(R), E_{K_{pub,m}}(M), (K_{pub,s})]$ 后用($K_{priv,m}$)解密 $E_{K_{pub,m}}(R)$,得到乱数 R; 解密 $E_{K_{pub,m}}(M)$,得到信息 M. 此时移动用户可用 M 作为初始值,输入A8得到通信密钥 K_c; 移动用户将随机数 R 以系统的公钥($K_{pub,s}$)加密得到 $E_{K_{pub,s}}(R)$,并将 $E_{K_{pub,s}}(R)$ 送给BS;BS 在收到 $E_{K_{pub,s}}(R)$ 后,用自己的私有密钥($K_{priv,s}$)解密得到随机数 R,与自己发送的随机数作比较,如果相同则为合法用户,将ACK 送给行动用户; 如果不同则为非法用户,移动用户与基站之间就以相同的密钥 K_c 进行通讯

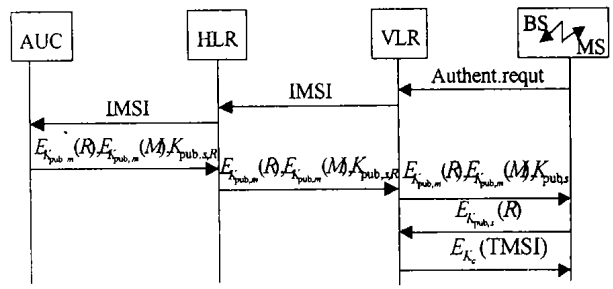

图2　基于 RSA 密码系统的 GSM 流程

该协议与 GSM 基本协议相比较虽实现了双方认证,使用公开加密算法RSA,但仍具有以下的不足之处:

1) 通讯方知道用户的真实身份,这是无线电子商务所不允许的,并且VLR 产生的临时身份对外部窃听者匿名,对公司内部无效

2) 加密算法唯一,不具有异类网的互操作性

3) 信道上传输的都是用公钥加密的数据,不具有不可抵赖性

4) HLR 负载过大, 每一次用户认证, 都需要与 HLR 通信, 这不仅造成信道传输量过大, 而且使 HLR 运转形成瓶颈

5) RSA 计算量大, 不适用于无线领域

3 基于椭圆曲线密码系统 GSM 网络身份认证协议的研究

3.1 基于 ECC 密码系统的 GSM 网络身份认证协议

椭圆曲线密码(ECC) 是基于有限域上椭圆曲线有理点群的一种密码系统 它的安全性基于有限域上椭圆曲线离散对数问题(ECDLP), ECDLP 比有限域上的离散对数问题(DLP) 要困难得多. 对于相同规模的参数, 椭圆曲线密码每一位密钥的强度要大得多. 173 比特的椭圆曲线系统相当于 1024 比特的 ElGamal 系统或 RSA 系统[4]. 可见椭圆曲线系统的参数规模要小得多, 而小的参数无论在实现上还是在应用上都具有较大的优越性 本文所用到数字签名、无逆方案数字签名以及密钥交换协议都是在椭圆曲线密码系统基础之上建立的 协议基本思想是: 为避免暴露通讯用户的真实身份给通讯服务方, 引入 CA 认证机构 用户和服务方首先要离线到 CA 处领取证书, 然后执行在线身份认证, 并引入各自相互签名方案, 传输的数据用私钥加密, 以防不可抵赖性 由于认证中多次用到数字签名, 因而使用无求逆签名方案[5], 减少了计算量

参数说明: E 为椭圆曲线, GF(P) 或 GF(2^k) 为椭圆曲线定义域; n 为椭圆曲线阶; P 为椭圆曲线一点

系统初始化:

密钥对的产生:

1) 随机选择一整数 $d \in [2, n-2]$;

2) 计算 $Q = d \times P$;

3) 椭圆曲线公钥为(E, P, n, Q), 私钥为 d.

3.1.1 用户和服务方获取证书

获取证书的协议流程如图 3 所示[6~9], 首先服务方选择密钥 d_s 计算公钥 Q_s, 并发送给认证机构 CA; 认证机构接到请求后, 为服务方产生签名密钥 K_s 和公钥 R_s, 并为服务方生成唯一标识 I_s, 接着完成椭圆曲线无逆签名操作, 生成签名数对(rs, ss); 发送证书公钥 Q_{ca}, 用户临识标识 I_s, 签名数对(rs, ss), 证书期限 T_s, 用户接收数据验证证书, 正确接收并

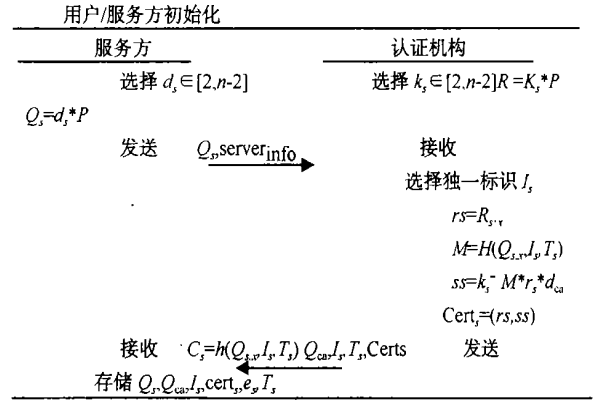

图 3 获取证书协议

存储 同样的过程适合于其他用户完成证书的获取过程(d_{ca} 为认证机构私钥). 该协议是离线执行的

3.1.2 用户和服务方相互认证

相互认证协议流程如图 4 所示, 此协议是在线执行的

(1) 首先用户向服务方发出呼叫请求, 传送临时身份标识 $I_{u,temp}$.

(2) 服务方接受临时身份标识, 并传向 HLR, 获取用户公钥, 同时向用户发出挑战数 g_s, 用户接收挑战数并产生自己的挑战数 g_u, 用椭圆曲线无逆签名算法对双方公钥及双方挑战数取哈希值, 再对哈希值签名

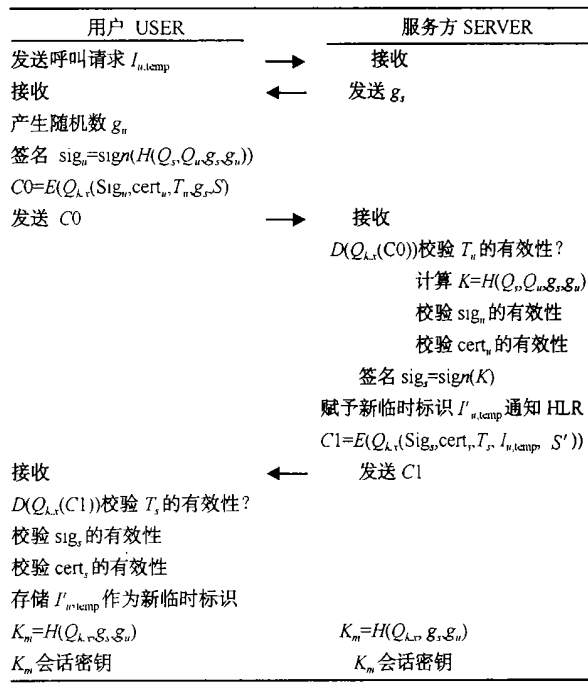

图 4 用户和服务方相互认证协议

(3) 用户用双方共同产生的密钥Q_{kx}作为默认对称加密算法的参数, 为如下数据加密: 数字签名 sig_u, 证书$cert_u$, 证书期限T_u, 挑战数g_u, 可供选择的加密算法S. 加密生成$C0$并传送给服务方.

(4) 服务方接受$C0$, 并对$C0$解密. 校验证书期限是否过期, 合格计算$K = H(Q_s, Q_u, g_s, g_u)$, 并用用户的公钥校验用户的数字签名 sig_u. 如果签名正确, 校验用户证书; 不正确, 终止. 否则, 对K进行服务方签名, 并赋予用户新的临识标识$I'_{u,temp}$, 选择会话密钥所使用的加密算法S', 并执行加密运算$C1 = E(Q_{kx}(sig_s, cert_s, T_s, I'_{u,temp}, S'))$. 传送$C1$给用户并计算双方通讯会话密钥$K_m = H(Q_{kx}, g_s, g_u)$.

(5) 用户解密$C1$验证服务方证书是否过期, 合格校验服务方数字签名, 校验证书并存储临时$I'_{u,temp}$标识, 生成会话密钥参数$K_m = H(Q_{kx}, g_s, g_u)$.

协议实现说明: 传递证书和签名而使用的加密函数$E()$, 其密钥为Q_{kx}, 加密算法为通讯双方的默认算法; 本协议假设 CA 机构颁发证书的信道是安全的, 例如可通过邮局传递, 或注册时传递给用户磁盘; $H()$函数为 SHA 算法; S 表示加密算法, S'表示算法类中的一种具体的加密算法.

3.2　协议安全分析

(1) 证书秘密性: 应用 D-H 密钥交换算法生成初始密钥, 保护互相认证过程中使用的数据, 并没有暴露证书内容.

(2) 前向加密: 会话密钥 K_m 是由一哈希函数作用生成, 即 $K_m = H$(参数集). 这样, 即使 K_m 丢失也不会使破译人员向后运行获取更多的重要信息, 如 Q_{kx}, g_u 等.

(3) 用户和服务器协商会话密钥, 此会话密钥将用于加密相互传输的数据. 在相互认证过程结束后, 双方都有一对新鲜随机挑战数 g_u 和 g_s 以及初始互认证密钥Q_{kx}. 由于只有 g_s 以明文形式传输, 所以窃听者只知道 g_s.

(4) 用户身份保密性: 在此协议中, 任何用户敏感数据永远不会暴露在开放环境中. 另外, 每次请求之后, 用户被赋予一个新的临时标识. 因此, 分析呼叫流量模式和临时身份不会对敌对者有帮助.

3.3　协议综合指标比较

下面就现有 GSM 认证协议、Lo and Chen 提出基于 RSA 密码系统 GSM 认证协议以及本文提出基于 ECC 密码系统 GSM 认证协议进行综合比较, 见表 1.

表 1　协议综合指标比较

指标	GSM 认证协议	Lo and Chen(基于 RSA)	本文 (基于 ECC)
认证安全性	差	好	好
速　度	快	慢	中等
密钥长度	固定长度且较短	可变长度(1024 位)	可变长度(320 位相当于 RSA 的 4096 位)
算　法	不公开	公开(购买)	公　开

4　结　　语

本文提出一个基于椭圆曲线密码系统(ECC)来解决 GSM 网络上身份认证的问题, 给出认证协议流程, 无论从安全性、认证性、防欺诈性以及密钥长度都比现有 GSM 及 Lo and Chen 提出的协议有诸多优点. 引入了 CA, 由 CA 颁发的证书, 与 HLR 无关, 避免了 Lo and Chen 协议对 HLR 的过分依赖性, 适合于无线数据网络(Bearer)带宽更窄的特点. ECC 密码系统, 更适合于移动终端的 CPU 功能较弱、小的存储器(ROM, RAM)、功耗受到一定限制的无线领域. 另外协议通过采用无逆签名方案大大减少标准化 ECDSA 的运算量, 使协议更适合无线网络和移动终端.

参考文献(References):

[1] Lo Chi-Chun, Chen Yu-Jen. A secure communication architecture for GSM networks [A]. *Proc IEEE PACRIM '99*[C]. Victoria, 1999.

[2] Lo Chi-Chun, Chen Yu-Jen. Secure communication mechanisms for GSM networks[J]. *IEEE Trans on Consumer Electronics*, 1999, 45(4): 1074-1080.

[3] Lo Chi-Chun, Chen Yu-Jen. Stream ciphers for GSM networks[J]. *Computer Communications*, 2001, 24(11): 1090-1096.

[4] 杨君辉, 戴宗铎, 杨栋毅, 等. 一种椭圆曲线签名方案与基于身份的签名协议[J]. 软件学报, 2000, 11(10): 1303-1306.

(下转第 480 页)

图2表明设置η可以控制查全率和查准率. η越大, $R_{\xi\alpha}$越大而$P_{\xi\alpha}$越小. 当η从0升到1, $R_{\xi\alpha}$也从0升到1, 而$P_{\xi\alpha}$从1减到0.7左右. 可以认为, 当$\eta=0$时, 所有的事件都会被检测为正常类型, 因此$R_{\xi\alpha}=0$而$P_{\xi\alpha}=1$; 当$\eta=1$时, 所有的事件都会被检测为攻击类型, 因此$R_{\xi\alpha}=1$而$P_{\xi\alpha}=0.7$左右. 注意到$R_{\xi\alpha}$的上升和$P_{\xi\alpha}$的减小都有一次突变, 分别在η为0～0.2之间和0.7～1之间. 可见, 选择η在0.2～0.7之间可以保证$R_{\xi\alpha}$和$P_{\xi\alpha}$都比较高.

5 结 论

本文提出一种控制SVM分类的查全率和查准率的方法, 并将其应用于异常检测系统中. 该方法利用在训练时SVM性能的可优化性, 通过GA优化SVM性能的同时, 调整反馈信息(即适应度)的表达式, 达到控制SVM的查全率和查准率的性能. 方法描述和实现包括3点: 1) 优化参数是特征选择和SVM训练模型的混合模型; 2) 查全率和查准率由$\xi\alpha$-estimate方法计算; 3) 期望的查全率和查准率由适应度表达式中的参数η控制. 实验结果表明随着η的增大, 查全率也增大而查准率却减小, 这样用户可以通过设置ρ的值来控制查全率和查准率.

参考文献(References):

[1] Lippman R P, Fried D J. Evaluating intrusion detectionsystems: The 1998 DARPA off-line intrusion detection evaluation[A]. *Proc of the DARPA Information Survivability Conf and Exposition*[C]. Hilton Head, 1999. 12-26.

[2] Denning E D. An intrusion detection Model[A]. *Proc of the IEEE Symposium on Security and Privacy*[C]. Oakland, 1986. 118-133.

[3] Vapnik V N. An overview of statistical learning theory[J]. *IEEE Trans on Neural Networks*, 1999, 10(5): 988-999.

[4] Yao X. Evolving artificial neural networks[J]. *Proc of the IEEE*, 1999, 87(9): 1423-1447.

[5] Holland J H. *Adaptation in Natural and Artificial Systems*[M]. Ann Arbor, Univ: Michigan Press, 1975.

[6] Smits G F, Jordaan E M. Improved SVM regression using mixtures of kernels[A]. *Proc of the* 2002 *Inter Joint Conf on Neural Networks*[C]. Honolulu, 2002. 3: 2785-2790.

[7] Osuna E, Freund R, Girosi F. Support vector machines: Training and applications[R]. Massachusetts Institute Technology, 1997.

[8] Joachims T. Estimating the generalization performance of a SVM efficiently[A]. *Proc of the Seventeenth Int Conf on Machine Learning*[C]. 2000. 431-438.

[9] The UCI KDD Archive. KDD Cup 1999 Data[EB/OL]. URL: http://kdd.ics.uci.edu/databases/kdducp99/kddcup99.html, 1999.

[10] Joachims T. SVM^{light} Support Vctor Machine[EB/OL]. URL: http://svmlight.joachims.org, 2002.

(上接第477页)

(YANG Junhui, DAI Zongduo, YANG Dongyi, et al. An elliptic curve signature scheme and an identity-based signature agreement[J]. *J of Software*, 2000, 11(10): 1303-1306.)

[5] 罗皓, 乔秦宝, 刘金龙, 等. 椭圆曲线签名方案[J]. 武汉大学学报(理学版), 2003, 149(11): 095-098.
(LUO Hao, QIAO Qinbao, LIU Jinlong, et al. Signing schedules with elliptic curve cryptography[J]. *J of Wuhan University*, 2003, 149(11): 095-098.)

[6] Microprocessor, Microcomputer Standards Committee of the IEEE Computer Society. IEEE Standard Specifications for Public Key Cryptography[DB/OL]. http://intl.ieeexplore.ieee.org. 2002-01-30.

[7] Sarbari Guta, Stephen M, Matyas J. Public key infrastructure analysis of existing and needed protocols and object formats for key recovery[J]. *Computers and Security*, 2000, 19: 56268.

[8] Park C-S. On certificate-based security protocols for wireless mobile communication systems[A]. *IEEE Network*[C]. 1997. 50-55.

[9] Beller M J, Chang L-F, Yacobi J. Privacy and authentication on a portable communications systems[J]. *IEEE J on Selected Areas in Communications*, 1993, 11(6): 821-829.