基于代理签名的移动通信网络匿名漫游认证协议

傅建庆*　陈　健　范　容　陈小平　平玲娣
(浙江大学新一代网络安全可控实验室　杭州　310027)

摘　要：随着无线移动终端的广泛应用，漫游认证、身份保密等问题显得日益突出。该文分析了现有的各种漫游认证协议在匿名性及安全性上存在的问题，指出现有协议都无法同时满足移动终端的完全匿名与访问网络对非法认证请求的过滤，进而针对性地提出了一种新的匿名认证协议。该协议基于椭圆曲线加密和代理签名机制，通过让部分移动终端随机共享代理签名密钥对的方式，实现了完全匿名和非法认证请求过滤。此外，协议运用反向密钥链实现了快速重认证。通过分析比较以及形式化验证工具AVISPA验证表明，新协议实现了完全匿名，对非法认证请求的过滤，双向认证和会话密钥的安全分发，提高了安全性，降低了计算负载，适用于能源受限的移动终端。

关键词：椭圆曲线加密；匿名；认证；代理签名
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2011)01-0156-07
DOI: 10.3724/SP.J.1146.2009.01455

A Delegation-based Protocol for Anonymous Roaming Authentication in Mobile Communication Network

Fu Jian-qing　Chen Jian　Fan Rong　Chen Xiao-ping　Ping Ling-di
(*New Generation Network Security Control Laboratory*, *Zhejiang University*, *Hangzhou* 310027, *China*)

Abstract: With the widespread use of mobile devices, issues like roaming authentication and identification privacy become increasingly prominent. This paper analyses the shortcomings of existing protocols of roaming authentication in term of anonymity and security that these protocols can not guarantee at the same time anonymity of mobile terminals and the filtration of illegal request. Based on elliptic-curve cryptography and proxy signature, a new anonymous protocol that allows a pair of proxy signature keys to be shared among some mobile devices randomly is proposed. Through analysis and verification using AVISPA, it shows that the new protocol realizes anonymity, the filtration of illegal request, mutual authentication and secure distribution of session key. It not only improves the security, but also reduces the computational load, which makes it more suitable for mobile devices with limited power.

Key words: Elliptic-curve cryptography; Anonymous; Authentication; Proxy signature

1　引言

在漫游环境中，移动终端(Mobile Station，MS)需要和访问网络完成相互认证才能开始进行通信。为了保护终端的隐私、防止网络窃听者的跟踪，需要在认证过程中隐藏终端的身份标识(Identity，ID)，需要做到(1)身份标识不能被获取；(2)不同的临时身份标识不能被确认是属于同一个移动终端[1]。此外，在匿名认证时，由于访问网络无法获知移动终端的任何身份信息，使得它无法及时识别非法移动终端、过滤非法认证请求，再加上无线网络本身的开放性，使得家乡网络更容易遭受诸如DOS等恶意攻击。因此，如何在匿名认证的同时实现访问网络对非法认证请求的过滤是亟待解决的问题。

第3代移动通信系统要求终端在其临时身份无法被识别时提供真实身份进行认证[2]，不满足完全匿名的第1项要求。文献[3–9]基于对称密钥加密，采用对ID进行加密或哈希的方式隐藏终端身份，但是它们都没有满足完全匿名的第2项要求，因为加密后的临时ID是长期不变的，而采用哈希方式获得的临时ID是前一个临时ID的哈希值。文献[10–13]基于非对称密钥加密，用家乡位置寄存器(Home Location Register，HLR)的公钥来加密MS的ID，从而实现了完全匿名，但无法过滤非法的认证请求。文献[14–16]基于非对称密钥加密实现了非法认证请求过滤，但是没有实现完全匿名[17]。

2009-11-11 收到，2010-10-15改回
国家863计划项目(2008AA01A323)，国家支撑计划项目(2008BA21B03)和浙江省科技计划(2007C11088，2008C210077)资助课题
*通信作者：傅建庆　Jianqing_fu@zju.edu.cn

本文基于椭圆曲线加密(Elliptic Curve Cryptography，ECC)[18]和代理签名机制[14]，提出了一种新的移动通信网络匿名漫游认证协议DARAP(Delegation-based Anonymous Roaming Authentication Protocol)，同时实现了移动终端身份隐藏和非法认证请求过滤。

2　相关技术介绍

本文提出的匿名认证协议主要采用了椭圆曲线加密技术和代理签名。椭圆曲线加密是一种低能耗的公钥加密技术，它建立在椭圆曲线离散对数的难解性问题之上。假设T，Q是椭圆曲线$EF(p)$上的点，其中T的阶为素数n，并且Q是T的倍数点，即存在$d \in N_n^*$，满足式(1)，那么椭圆曲线离散对数的难解性问题就是指通过T，Q很难确定d。于是可以公开Q作为公钥，保留d作为私钥。相比普通的公钥加密算法，ECC拥有密钥长度小、安全性能高、数字签名耗时小等特点，在智能终端(比如掌上电脑、移动手机)应用中有很大的发展潜力。

$$Q = dT \tag{1}$$

代理签名的基本原理是：HLR把自己的公、私钥相关信息授权给MS用于签名，当访问位置寄存器(Visitor Location Register，VLR)得到MS的签名消息后，就可以用HLR的公钥对消息进行验证，从而验证MS的合法性。在此过程中，MS不需要提供真实的身份标识。DARAP中采用代理签名的主要目的是在保证MS身份隐藏的前提下实现访问网络对MS的初步认证。

3　基于代理签名的匿名认证

3.1 初始化过程

初始化过程主要完成MS在HLR上的注册，HLR将在注册过程中为MS分配代理签名密钥对。假设家乡网络的HLR拥有非对称密钥对(d,Q)满足式(1)，它的具体操作如下：

(1)随机生成小于q的正整数k(q为小正整数)，计算代理密钥对(a,B)，过程如下：

$$B = kT \tag{2}$$

$$a = d \cdot h(\theta(B)) + k \tag{3}$$

其中$\theta(\cdot)$是一个把椭圆曲线$EF(p)$上的点映射到字符串的函数，$h(\cdot)$是一个把字符串映射到整数的单向哈希函数。由于k的值域为小整数范围，使得(a,B)较容易重复，随机被多个节点共享。主要目的防止攻击者根据MS的代理公钥进行跟踪，相关的安全性问题将在3.5节中详细分析。

(2)随机生成正整数rand，利用伪随机法[19]计算MS的临时身份IDMA如下：

$$\text{IDMA} = [\text{IDM} \mid \text{rand}]K_H \tag{4}$$

(3)产生随机数$K_{H,M}$作为HLR和MS之间的共享密钥。

(4)产生随机数seq，作为HLR和MS保持认证同步用的序列号。

(5)把$(\text{IDMA}, a, B, K_{H,M}, \text{seq})$安全地传递给MS。保存$K_{H,M}$和seq，丢弃IDMA, a, B。

3.2 HLR在线认证过程

HLR在线认证过程如图1所示，具体步骤如下：

步骤1　MS生成消息S1，并发送给VLR。

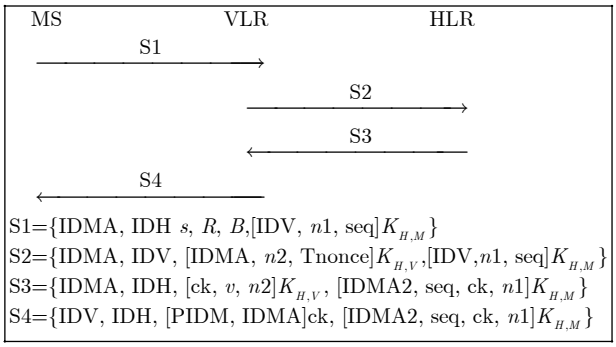

图1 DARAP的HLR在线认证过程

(1)MS接收VLR定期广播的随机数Nonce，随机选择正整数m，生成签名认证信息(s,R)如下：

$$R = mT \tag{5}$$

$$s = a \cdot h(\theta(R) \mid \text{Nonce} \mid \text{IDMA}) + m \tag{6}$$

(2)随机产生正整数$n1$；

(3)更新本地seq为seq + 1；

(4)组成消息S1={IDMA, IDH, s, R, B, [IDV, $n1$, $K_{H,M}$}，发送给VLR。

步骤2　VLR验证消息S1，并向HLR发送消息S2。

(1)VLR验证(s,R)有效性，检验下式是否成立：

$$sT = (h(\theta(B))Q + B) \cdot h(\theta(R) \mid \text{Nonce} \mid \text{IDMA}) + R \tag{7}$$

(2)随机产生正整数$n2$；

(3)生成时间戳Tnonce；

(4)组成消息S2 = {IDMA, IDV, [IDMA, $n2$, Tnonce]$K_{H,V}$, [IDV, $n1$, seq]$K_{H,M}$}，发送给HLR。

步骤3　HLR验证消息S2，并向VLR发送消息S3。

(1)HLR解密IDMA得到MS的真实身份IDM，并根据MS的真实身份从本地数据库获取到它们之间的共享密钥$K_{H,M}$；

(2)用$K_{H,M}$解密得到IDV, $n1$, seq；

(3)确认解密得到的seq大于本地保存值，然后

更新至本地seq；

(4)根据解密得到的IDV，获取共享密钥$K_{H,V}$，解密$[\mathrm{IDMA},n2,\mathrm{Tnonce}]K_{H,V}$；

(5)验证解密得到的IDMA是否和接收到的IDMA一致；

(6)确认解密得到的Tnonce的有效性；

(7)计算MS和VLR之间的会话密钥

$$\mathrm{ck}=h(K_{H,M}\mid K_{H,V}\mid \mathrm{IDMA}\mid \mathrm{IDV}\mid n1\mid n2) \quad (8)$$

(8)重新随机生成正整数rand，按照公式(4)为MS生成新的临时身份，并保存为IDMA2；

(9)计算重认证验证信息v，用于VLR在重认证过程中认证MS

$$v=h^{t+1}(K_{H,M}\mid \mathrm{ck}) \quad (9)$$

其中t是出于安全考虑而限定的最大重认证次数，本文假定$t\le 10$；

(10)组成消息$\mathrm{S3}=\{\mathrm{IDMA},\mathrm{IDH},[\mathrm{ck},v,n2]K_{H,\mathrm{V}},[\mathrm{IDMA2},\mathrm{seq},\mathrm{ck},n1]K_{H,M}\}$，发送给VLR。

步骤4 VLR接收消息S3，并向MS发送消息S4。

(1)VLR用密钥$K_{H,V}$解密得到$\mathrm{ck},v,n2$；

(2)确定$n2$的有效性，即$n2$为本次认证过程中VLR产生的随机数；

(3)保存会话密钥ck以及重认证信息v；

(4)生成随机数rand2，用伪随机法计算MS在访问域的临时身份PIDM并保存

$$\mathrm{PIDM}=[\mathrm{IDMA}|\mathrm{rand2}]K_V \quad (10)$$

(5)组成消息$\mathrm{S4}=\{\mathrm{IDV},\mathrm{IDH},[\mathrm{PIDM},\mathrm{IDMA}]\mathrm{ck},[\mathrm{IDMA2},\mathrm{seq},\mathrm{ck},n1]K_{H,M}\}$，发送给MS。

步骤5 MS接收消息S4。

(1)用$K_{H,M}$解密得到IDMA2,seq,ck,$n1$；

(2)确定$n1$的有效性，即确认$n1$为本次认证过程中MS产生的随机数；

(3)确认seq的有效性；

(4)保存解密得到的IDMA2，用作下次HLR在线认证的临时ID；

(5)保存解密得到的会话密钥ck；

(6)用ck解密得到PIDM,IDMA；

(7)验证IDMA的完整性，以此确定[PIDM, IDMA]ck这部分内容没有被篡改，从而确认PIDM的完整性；

(8)保存PIDM，用作MS在访问域的临时ID。

3.3 快速重认证过程

当MS完成HLR在线认证后，MS和VLR之间共享了会话密钥ck。在ck过期之前，MS可以向VLR提出重认证，以更新会话密钥，延长接收服务的时间。为了加快认证，减轻HLR负担，重认证过程由MS和VLR独立完成。快速重认证过程中用到了反向哈希链技术，用于VLR对MS的认证。MS进行第i次快速重认证的过程如图2所示，具体步骤如下：

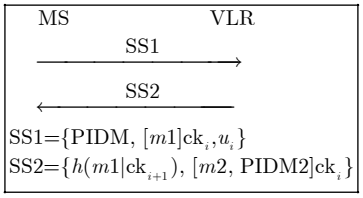

图2 DARAP第i次快速重认证过程

步骤1 MS发送消息SS1给VLR。

(1)MS查看本地是否存在哈希链$h(K_{H,M}\mid \mathrm{ck})$, $h^2(K_{H,M}\mid \mathrm{ck}),\cdots,h^t(K_{H,M}\mid \mathrm{ck})$，不存在则生成之；

(2)从哈希链中获取$u_i=h^{t+1-i}(K_{H,M}\mid \mathrm{ck})$；

(3)随机产生$m1\in N^*$；

(4)组成消息$\mathrm{SS1}=\{\mathrm{PIDM},[m1]\mathrm{ck}_i,u_i\}$，发送给VLR，其中$\mathrm{ck}_i$是当前使用的会话密钥，$\mathrm{ck}_1=\mathrm{ck}$。

步骤2 VLR核对消息SS1，并发送消息SS2给MS。

(1)VLR获取本地保存的重认证验证信息v，验证$v=h(u_i)$是否成立。验证通过则更新$v=u_i$；

(2)用当前会话密钥解密获得$m1$；

(3)产生随机数$m2\in N^*$；

(4)计算新的会话密钥

$$\mathrm{ck}_{i+1}=h(\mathrm{ck}_i\mid \mathrm{PIDM}\mid \mathrm{IDV}\mid m1\mid m2\mid u_i) \quad (11)$$

(5)按照式(10)为MS生成新的临时身份PIDM2；

(6)组成消息$\mathrm{SS2}=\{h(m1\mid \mathrm{ck}_{i+1}),[m2,\mathrm{PIDM2}]\mathrm{ck}_i\}$，发送给MS。

步骤3 MS核对消息SS2。

(1)用当前会话密钥解密得到$m2,\mathrm{PIDM2}$；

(2)按照式(8)计算新的会话密钥ck_{i+1}；

(3)计算$h(m1\mid \mathrm{ck}_{i+1})$进行匹配，确认收到消息的有效性；

(4)保存PIDM2，用作MS在访问域的新的临时身份。

4 安全性分析

4.1 完全匿名

本文在HLR在线认证和快速重认证过程中都采用伪随机方式[19]对MS的身份进行匿名保护。在HLR在线认证过程中，HLR通过式(4)将MS的真实身份信息隐藏其中，只有知道K_H才能得到MS的真实身份，所以只有HLR才能得到识别MS。在快速重认证过程中，VLR通过式(10)将MS的真实身份信息隐藏其中，只有知道K_V才能得到MS的真实身份，所以只有VLR才能识别MS。因此，在整个协议过程都实

现了移动终端的身份隐藏。

此外，由于在HLR在线认证和快速重认证过程中，MS每次使用的临时ID都不相同，式(4)和式(10)中的两个随机数rand和rand2保证了每个临时ID之间没有依赖关系，从而使得攻击者无法辨别两个不同的临时ID是否属于同一个MS，防止了攻击者的身份跟踪，从而实现了完全的匿名。

4.2 认证请求过滤

认证请求过滤发生在HLR在线认证的过程中，当VLR接收到消息S2时，它通过式(7)来验证签名信息(s,R)的正确性，从而实现对MS的认证。结合式(1)-式(6)，式(7)的计算过程如式(12)所示。

由此可知，合法的MS的确能够通过VLR的认证，只需证明非法的MS无法生成正确的(s,R)即可。假设非法MS能够生成满足式(7)的(s,R)，那么它要么先指定s，要么先指定R。

$$\begin{aligned} sT &= a\cdot h(\theta(R)\mid \text{Nonce}\mid \text{IDMA})T + mT \\ &= (d\cdot h(\theta(B))+k)\cdot h(\theta(R)\mid\text{Nonce}\mid\text{IDMA})T + mT \\ &= (dT\cdot h(\theta(B)) + kT)\cdot h(\theta(R)\mid \text{Nonce}\mid \\ &\quad \text{IDMA})T + mT = (h(\theta(B))Q + B)\cdot h(\theta(R) \\ &\quad \mid \text{Nonce}\mid \text{IDMA}) + R \end{aligned} \tag{12}$$

如果它先指定s，假设$s=1$，则需要寻找R来满足等式$(h(\theta(B))Q+B)\cdot h(\theta(R)\mid \text{Nonce}\mid \text{IDMA})+R=T$，即$R=((d\cdot h(\theta(B))+k)\cdot h(\theta(R)\mid \text{Nonce}\mid\text{IDMA})-1)T$，显然等式右边是$T$的一个倍点，因此$R$是$T$的一个倍点，可以设$R=qT\ \ (q\in N_n^*)$，那么等式转换为$qT=((d\cdot h(\theta(B))+k)\cdot h(\theta(qT)\mid \text{Nonce}\mid\text{IDMA})-1)T$，其中等式右边为椭圆曲线$EF(p)$上的一个不定点。由椭圆曲线上的离散对数难解性可知，即使等式右边是个定点也难以求出整数q，更何况它是不定点。

如果它先指定R，假设$R=T$，那么等式转换为$sT=(h(\theta(B))Q+B)\cdot h(\theta(T)\mid \text{Nonce}\mid\text{IDMA})+T$，其中右边为椭圆曲线$EF(p)$上的一个定点，由椭圆曲线上的离散对数难解性可知，难以求出满足等式的s。

综上所述，非法的MS无法生成正确的(s,R)。此外，注意到验证(s,R)过程中引入了VLR周期发布的随机数Nonce，可以在防止恶意节点的重放攻击。

4.3 双向认证

在HLR在线认证过程中，MS和VLR之间的相互认证是在HLR的帮助下完成的，主要借助MS和HLR以及VLR和HLR之间的相互认证来实现。

MS在发送的消息S1中附带了自身产生的随机数$n1$，并和其它参数一起用共享密钥$K_{H,M}$进行了加密。在接收到消息S4后，MS验证其中是否包含了用$K_{H,M}$加密的$n1$，由此来实现对HLR的认证。而HLR通过检验用共享密钥$K_{H,M}$加密的seq是否正确来认证MS。

VLR在发送的消息S2中附带了自身产生的随机数$n2$，并和其它参数一起用共享密钥$K_{H,V}$进行了加密。在接收到消息S3后，VLR验证其中是否包含了用$K_{H,V}$加密的$n2$，由此来实现对HLR的认证。而HLR通过检验用共享密钥$K_{H,V}$加密的时间戳Tnonce的时效性来认证VLR。

在进行快速重认证中引入了反向哈希链技术，MS从哈希链$h(K_{H,M}\mid \text{ck}),h^2(K_{H,M}\mid \text{ck}),\cdots,h^t(K_{H,M}\mid \text{ck})$的末尾开始从后往前取值，每次重认证都取一项发给VLR进行验证，并且每项只使用一遍。由哈希函数的单向性可知，只有拥有$K_{H,M}$和ck的终端才能计算该哈希链，才能发送合法的重认证请求，因此对方只能是MS或HLR，又由于HLR不参与认证，因此对方必定是MS。由此VLR成功认证了MS。另一方面，MS接收到的消息SS2中包含了哈希以后的$m1$，而$m1$是此前MS随机产生并用ck_i加密后发送的，因此只有拥有ck_i才能得到$m1$，对方一定是正确的VLR。由此MS完成了对VLR的认证。

4.4 会话密钥分发

在HLR在线认证过程中，MS收到了消息S4，其中包含了用$K_{H,M}$加密的会话密钥ck，因为MS拥有密钥$K_{H,M}$，所以它能解密得到ck。此外消息S4中包含了用ck加密的IDMA，由IDMA的完整性可知VLR的确获知了ck。因此，MS，VLR的确获得了会话密钥。另一方面，MS在消息S1中加密指定了IDV，VLR在消息S2中加密指定了IDMA，这确保了HLR能够使用正确的IDV和IDMA以及正确的$K_{H,M}$和$K_{H,V}$计算会话密钥。由于计算会话密钥需要拥有$K_{H,M}$和$K_{H,V}$，因此只有HLR有此能力。其它节点要获取ck只能通过解密消息S3或S4，而这两个消息中会话密钥用$K_{H,M}$或$K_{H,V}$进行了加密，仅HLR，VLR和MS有能力解密，从而确保了仅HLR，VLR和MS有能力获取到会话密钥ck。综上所述，有且仅有MS，VLR和HLR拥有ck，会话密钥得到了安全分发。

在重认证过程中，MS收到的消息SS2中包含了用ck_i加密的随机数$m2$，由此MS可以计算得到新的会话密钥ck_{i+1}。通过验证$h(m1\mid \text{ck}_{i+1})$的正确性可知，VLR也获得了$\text{ck}_{i+1}$。因此，MS，VLR的确获得了新的会话密钥$\text{ck}_{i+1}$。另一方面，式(11)表明，计算新的会话密钥$\text{ck}_{i+1}$需要拥有随机数$m1$和$m2$，而$m1$，$m2$都是用会话密钥$\text{ck}_i$加密后发送的，因此只有MS，VLR和HLR有能力计算ck_{i+1}。由于HLR

不参与重认证，故有且仅有MS和VLR拥有 ck_{i+1}，会话密钥得到了安全分发。

4.5 代理签名密钥对共享

在HLR在线认证过程中，VLR使用MS的代理公钥和HLR的公钥对认证请求进行验证。本文让部分MS随机共享相同的代理密钥对，主要原因有4点：(1)代理公钥无法事先发布，MS必须把它附带在认证请求中；(2)不能给MS的分配唯一的代理密钥对，否则无法防止攻击者根据代理公钥跟踪MS；(3)不能给所有MS分配相同的代理密钥对，否则一旦其中一对被破解就需要进行全局的更新；(4)不能按照特定的规则给MS分配相同的代理密钥对，否则就能在一定程度上根据代理公钥区分MS，实现身份跟踪。

随机共享代理密钥对本身也是安全的，原因有3点，(1)对于VLR而言，它只需要知道MS是否是HLR的合法用户，相同的代理公钥并不影响它的判断；(2)对于非恶意的MS而言，这也不影响它的签名使用；(3)对于恶意的MS而言，由于最终需要HLR来确认MS的身份合法性，使得它实际上无法伪装成其它的合法MS；此外，它也不需要伪装成其它合法MS来通过VLR的验证，因为它本身就拥有合法的代理密钥对；更重要的是，由于代理密钥对只被用于签名认证，不用于信息加密，从而使得恶意的MS无法根据相同的代理密钥对去获取有效信息。

5 基于AVISPA的安全性形式化证明

由于无线移动通信网络的开放性，攻击者可以非常容易地窃听、拦截、修改甚至添加消息，这类攻击一般被称为Dolev-Yao攻击。为了模拟Dolev-Yao攻击，本文选取支持Dolev-Yao攻击模型的安全协议验证工具Automated Validation of Internet Security Protocols and Applications (AVISPA)[20]来验证HLR在线认证的安全性。AVISPA使用形式化语言高级协议规范语言(High Level Protocol Specification Language，HLPSL)来描述协议，并使用4个安全验证模型来验证协议的安全性。4个验证模型分别是动态模型检验器(OFMC)，基于逻辑为约束的攻击搜索器(CL-AtSe)，基于SAT的模型检验器(SATMC)，以及基于自动逼近的树自动机安全协议分析(TA4SP)。

HLR在线认证的安全目标主要包括MS和VLR之间的相互认证以及会话密钥的安全分发。其中MS和VLR之间的相互认证主要借助MS和HLR以及VLR和HLR之间的相互认证来实现。会话密钥的安全分发是指仅MS，VLR和HLR获得了会话密钥，攻击者无法窃取。安全目标的AVISPA代码如图3所示。

```
goal
    secrecy_of ck                          %需要保证ck不被泄露
    authentication_on ms_hlr_n1            %MS需要通过n1来
                                           认证HLR
    authentication_on vlr_hlr_n2           %VLR需要通过n2
                                           来认证HLR
    authentication_on hlr_vlr_tnonce       %HLR需要通过
                                           Tnonce来认证VLR
    authentication_on hlr_ms_seq           %HLR需要通过
                                           seq来认证MS
end goal
```

图3 安全目标的AVISPA代码

AVISPA采用类似有限状态机的方法来描述参与协议的各个节点。由于它无法表示时间戳和序号seq的同步检测，本文假设在认证开始之前，HLR已经秘密地将认证时需要用到的时间戳转交给了VLR，将序号seq转交给了MS。各个节点的状态转换过程如图4所示，限于篇幅，省略具体验证代码。

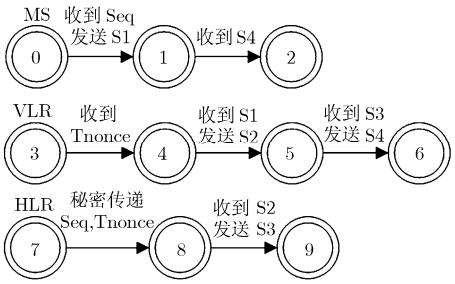

图4 DARAP HLR在线认证过程中的状态转换图

最终，通过AVISPA在线验证工具(http://www.avispa-project.org/)验证。OFMC，CL-AtSe以及SATMC验证模型的表示DARAP的HLR在线认证过程是安全的，而TA4SP验证模型表示它无法模拟协议。

6 计算负载比较

本节将比较各种协议中MS的计算负载，鉴于DARAP的主要贡献在于同时实现了匿名认证和非法认证请求过滤，因此只与实现了非法认证请求过滤的匿名认证协议[14,16]进行比较(文献[15]完全被包括在文献[16]中，此处不进行比较)。

表1描述了各种协议中MS的计算负载，其中 t^- 表示小于 t。可见DARAP进行HLR在线认证需要1次哈希计算，3次共享密钥加解密计算和1次椭圆曲线密钥签名认证计算，进行快速重认证需要2至 $t+1$ 次哈希计算、2次对称密钥签名认证和1次对称密钥

加解密计算。其中，t 次哈希计算是计算反向哈希链产生的，被平摊到多次重认证后，平均每次重认证最少需要进行1次哈希操作，最多 t 次。根据本文假设，$t \le 10$，因此平均每次重认证最多进行10次哈希操作。

表 1 各种协议中 MS 进行的各项计算次数

		哈希计算	对称密钥加解密	普通公钥签名认证	椭圆曲线密钥签名认证
文献[14]	HLR在线认证	1	1	1	0
	快速重认证	3	1	0	0
文献[16]	HLR在线认证	1	3	0	1
	快速重认证	1	0	0	1
DARAP	HLR在线认证	1	3	0	1
	快速重认证	$t^{-}+1(t \le 10)$	2	0	0

由于哈希运算的平均速度是对称密钥加/解密的100倍，而对称密钥加/解密的速度是公钥签名/认证的100倍[14]，再加上椭圆曲线加密的计算复杂度远小于普通公钥加密，所以DARAP进行HLR在线认证的计算量小于文献[14]，和文献[16]几乎一致，进行快速重认证时的计算量略大于文献[14]，远小于文献[16]。综合来说，DARAP的计算负载小于文献[14]和文献[16]。此外，由于文献[14]在快速重认证过程中，MS并没有实现对VLR的认证，因此DARAP在快速重认证中的计算量是可取的。

7 结束语

本文通过对现有的各种无线匿名认证协议的分析，指出了现有协议存在的不足，即不能同时实现完全匿名和非法认证请求过滤，从而针对性地提出了一个新的无线匿名认证协议DARAP。协议在解决该问题的同时也降低了移动终端的计算负载，从而使得其更适用于能源受限的移动终端。

尽管如此，DARAP还有诸多方面可以改进，比如：家乡网络没有充分利用访问网络对移动终端的认证结果，而是重新对移动终端进行认证。今后的研究目标是在实现身份隐藏和非法认证请求过滤的基础上，充分利用访问网络对移动终端的认证结果来减轻家乡网络的工作负担，并尝试进一步减少移动终端的计算负载。

参 考 文 献

[1] Kesdogan D and Palmer C. Technical challenges of network anonymity[J]. *Computer Communications*, 2006, 29(3): 306–324.

[2] 3GPP TS 33.102 V8.1.0. Policy and charging control architecture[S]. Release 8, 2008–12.

[3] Wu Chia-chun and Lee Wei-bin, *et al.*. A secure authentication scheme with anonymity for wireless communications[J]. *IEEE Communications Letters*, 2008, 12 (10): 722–723.

[4] 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.
Zhu Jian-ming and Ma Jian-feng. An efficient authentication protocol with anonymity for wireless IP networks[J]. *Journal of China Institute of Communication*, 2004, 259(6): 12–18.

[5] Zhu Jian-ming and Ma Jian-feng. A new authentication scheme with anonymity for wireless environment[J]. *IEEE Transactions on Consumer Electronic*, 2004, 50(1): 231–235.

[6] Lee J S and Chang J H. Security flaw of authentication scheme with anonymity for wireless communications[J]. *IEEE Communications Letters*, 2009, 13(5): 292–293.

[7] Wong D S. Security analysis of two anonymous authentication protocols for distributed wireless networks[C]. Third IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, Hawaii, USA, 2005: 284–288.

[8] Zeng Peng and Cao Zhen-fu, *et al.*. On the anonymity of some authentication schemes for wireless communications[J]. *IEEE Communications Letters*, 2009, 13(3): 170–171.

[9] Wei Yong-zhuang and Qiu Hong-bing, *et al.*. Security analysis of authentication scheme with anonymity for wireless environments [C]. International Conference on Communication Technology, Guilin, China, 2006: 1–4.

[10] He Q, Wu D, and Khosla P. The Quest for personal control over mobile location privacy[J]. *IEEE Communications Magazine*, 2004, 42(5): 130–136.

[11] Molva R, Samfat D, and Tsudik G. Authentication of mobile users[J]. *IEEE Network, Special Issue on Mobile Communications*, 1994, 8(2): 26–34.

[12] Neuman B C and TS'O T. Kerberos: an authentication service for computer networks[J]. *IEEE Communications Magazine*, 1994, 32(9): 33–38.

[13] 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.
Peng Hua-xi and Feng Deng-guo. An efficient authentication protocol with anonymity for wireless IP networks [J]. *Journal of China institute of Communication*, 2006, 27(9): 78–85.

[14] Lee Wei-bin and Chang-Kuo Y. A new delegation-based authentication protocol for use in portable communication systems[J]. *IEEE Transactions on Wireless Communications*,

2005, 4(1): 57–64.

[15] Tang Cai-mu and Wu D O. An efficient mobile authentication scheme for wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(4): 1408–1416.

[16] Tang Cai-mu and Wu D O. Mobile Privacy in Wireless Networks-Revisited[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(3): 1035–1042.

[17] Fu Jian-qing, Chen Jian, and Fan Rong, *et al.*. An efficient delegation-based anonymous authentication protocol[C]. Second International Workshop on Computer Science and Engineering, Qingdao, China, 2009, 1: 558–562.

[18] Johnson D, Menezes A, and Vanstone S. The elliptic curve digital signature algorithm (ECDSA)[J]. *International Journal of Information Security*, 2001, 1(1): 36–63.

[19] Ateniese G, Herzberg A, and Krawczyk H, *et al.*. Untraceable mobility or how to travel incognito[J]. *Computer Networks*, 1999, 31(8): 785–899.

[20] Bozga L, Lakhnech Y, and Perin M. Hermes: An automatic tool for the verification of secrecy in security protocols[C]. 15th International Conference on Computer Aided Verification, Colorado, USA, 2003, 2725: 219–222.

傅建庆： 男，1982年生，博士生，研究方向为无线网络安全、下一代网络安全.

陈　健： 男，1962年生，副研究员，研究方向为网络信息安全、模式识别.

范　容： 男，1981年生，博士生，研究方向为无线传感器网络安全.

陈小平： 男，1963年生，副教授，研究方向为计算机应用、计算机网络应用、信息安全.

平玲娣： 女，1946年生，教授，博士生导师，研究方向为网络信息安全、安全操作系统、可信计算与安全语言、下一代网络通讯与分布处理技术.