直接匿名的无线网络可信接入认证方案

杨力[1,2]，马建峰[1,2]，裴庆祺[2]，马卓[1]

（1. 西安电子科技大学 计算机学院，陕西 西安 710071；

2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：基于直接匿名证明思想，提出一种无线移动网络中移动用户可信接入认证方案，认证移动用户身份的同时利用直接匿名证明方法验证平台身份的合法性和可信性。方案中，外地网络代理服务器直接验证移动用户平台可信性，并与本地网络代理服务器一同验证移动用户身份，采用临时身份和一次性密钥，保持用户身份匿名性。分析表明，方案具有域分离特性和密钥协商公正性，性能满足无线移动网络环境安全需求。

关键词：无线网络；认证；匿名；可信计算；远程证明

中图分类号：TN918.1 **文献标识码**：B **文章编号**：1000-436X(2010)08-0098-07

Direct anonymous authentication scheme for wireless networks under trusted computing

YANG Li[1,2], MA Jian-feng[1,2], PEI Qing-qi[2], MA Zhuo[1]

(1. School of Computer Science, Xidian University, Xi'an 710071, China;

2. Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: Based on direct anonymous attestation of trusted computing, a wireless anonymous authentication scheme was proposed, the platform of the mobile node was verified by the foreign network agent and the identity of the mobile node user was authenticated by the home network agent and the foreign network agent together. By using of temporary identities and one time secret keys, identity anonymity and domain separation property are achieved. The analysis shows that the scheme is secure, reliable, and with higher performance.

Key words: wireless networks; authentication; anonymity; trusted computing; remote attestation

1 引言

无线网络技术不断发展，移动终端设备越发普及，可以方便地接入互联网以获取服务。无线网络传输媒体的开放性使得在无线网络环境下，有线环境的安全威胁和针对无线环境的安全威胁并存[1]。无线移动网络中，用户认证是整个安全方案的基础，匿名性是无线网络认证方案的重要方面，在认证的同时，尤其是移动节点在无线网络中进行漫游认证时，需要提供匿名服务来隐藏移动节点的真实身份，以保护节点用户隐私。

典型的无线匿名认证协议[2~5]只认证用户身份，缺乏对用户平台的验证，存在一定安全隐患，不适用于移动电子商务、数字版权管理等高安全需

收稿日期：2010-01-27；**修回日期**：2010-07-01

基金项目：国家高技术研究发展计划（"863"计划）基金资助项目（2007AA01Z429）；国家自然科学基金资助项目（60633020, 60872041, 60803150）；国家自然科学基金委员会—广东联合基金重点基金资助项目(U0835004)

Foundation Items: The National High Technology Research and Development Program of China(863 Program) (2007AA01Z429)；The National Natural Science Foundation of China (60633020,60872041,60803150)；The Key Program of NSFC-Guangdong Union Foundation (U0835004)

求的无线服务提供领域。移动终端设备存储资源和计算资源有限，其系统本身面临诸多安全威胁，即使用户身份合法，不表示其使用的平台安全可信。移动终端平台的安全是获得安全服务的前提和保障，一旦用户平台未能按照约定处于某安全配置状态，如存在软件安全漏洞、软件版本过期等，会给所登录的服务器造成安全危害。

可信计算理论和相关技术，其初衷是为了从终端平台结构上解决安全问题，提供和加强对终端平台系统的验证和保护，相应的技术规范由可信计算组织(TCG, trusted computing group)[6]提出，已逐渐被学术界和产业界所接受，成为当前信息安全领域研究的热点[7,8]。

目前，可信计算环境下，无线移动网络接入认证问题已有一定的研究。文献[9]提出一种基于可信计算的移动终端用户认证方案，实现了用户与可信移动终端的相互认证，但未解决移动用户和移动平台作为整体接入网络的问题。基于 TCG 可信平台模块(TPM, trusted platform module)规范 v1.1b[10]，作者曾提出可信计算环境下用户利用可信移动终端接入网络进行身份认证和平台验证的无线网络可信匿名认证方案[11]，方案借助 TCG 规范中的可信第三方隐私 CA(privacy-CA)，并将平台信息发回给本地网络以完成平台身份和可信性验证，但需要转发的消息量较多且不具有直接匿名性。

基于可信计算直接匿名证明的思想，本文提出一种可信计算环境下无线移动网络中移动节点直接匿名的接入认证方案，在认证移动用户身份的同时利用远程证明方法验证平台身份合法性和可信性。认证过程中，外地网络代理服务器直接验证移动用户平台可信性，并与本地网络代理服务器一同验证移动用户身份，移动用户与本地网络及外地网络交互的每阶段使用不同的临时身份和一次性密钥，保持用户身份匿名，且使得方案具有域分离特性和密钥协商公正性。考虑到移动设备运算能力和通信带宽有限，协议交互过程中主要采用散列运算、对称加密与对称解密运算，且部分计算量由可信平台模块完成，协议计算代价和消息交互轮数均满足无线移动网络环境安全需求。

本文结构安排如下：第 2 节简要介绍可信计算的远程证明理论，第 3 节给出方案实现的可信环境下的无线移动网络模型，第 4 节描述方案的详细过程，第 5 节分析方案的安全性和性能，第 6 节是本文的结束语。

2　背景知识

可信计算技术的核心是在终端平台上嵌入可信平台模块 TPM，作为独立的安全协处理芯片提供密码支持和有保护的存储功能，为各种可信机制和安全功能提供硬件保障，为度量和验证平台的可信属性提供基础。

TPM 具有远程证明（RA, remote attestation）的能力，包括对 TPM 即平台身份的证明和对平台完整性的证明，具体地，通过交互协议证明平台身份，通过完整性验证证明平台可信性。对于身份证明，TCG 先后提出 2 种解决方案，分别是引入可信的第三方即隐私 CA（privacy-CA）的方案和直接匿名证明（DAA, direct Anonymous attestation，）方案[12]。在 Privacy-CA 方案中，Privacy-CA 作为权威证书机构向 TPM 颁发身份证书，当 TPM 向验证方证明身份时出示该证书，验证方将证书返回给 Privacy-CA 并与其一同验证 TPM 的合法性。由于每次进行证明时都需要 Privacy-CA 的参与，会成为系统的安全和性能瓶颈。

为克服此缺陷，TPM 规范 v1.2 中采纳了 Brickell 等提出的直接匿名证明方法，简称 BCC 方案。BCC 方案基于 CL 群签名[13]和知识证明方法构建，使得 TPM 在向远程验证方证明身份的同时不泄露隐私信息。但是，在 BCC 方案中，TPM 及所在平台与验证者交互复杂且运算量大，不适用于计算资源有限的嵌入式设备。He 等人提出能够满足嵌入式系统的直接匿名证明方案[14]，简称 DAA-ED 方案。该方案基于 CM 群签名方案[15]设计，简化了 TPM 及平台与验证方的交互复杂度，缩减了协议运算量，解决了资源受限环境下的 TPM 直接匿名证明问题，适用于移动计算平台等资源受限系统。本文所提出方案中，对平台身份的认证采用此方法来设计，达到平台身份的直接匿名证明。

3　协议模型框架

方案的无线移动网络模型如图 1 所示。

合法的 TPM 在制造商所在网络加入 DAA 颁发者群，并取得其 DAA 证书。移动节点（MN）是嵌入了合法 TPM 芯片的可信无线终端设备，MN 以无线方式接入网络。本地网络、外地网络与制造商所在网络以有线的方式连接，并通过各自的网络连接设备如路由器连接到 Internet，且本地网络代理（HA）

和外地网络代理（FA）已通过安全的方式获知 DAA 颁发者的公开参数。在本地网络（HN）中，MN 通过本地网络代理（HA）接入网络。MN 接入本地网络时，HA 对其进行身份认证和平台验证，确认 MN 的身份合法性与平台可信性。当 MN 漫游至外地网络（FN）时，通过外地网络代理（FA）接入网络，FA 直接对 MN 的平台身份和完整性进行验证，并通过 HA 对 MN 进行身份认证。STA 为网络中的其他工作站。

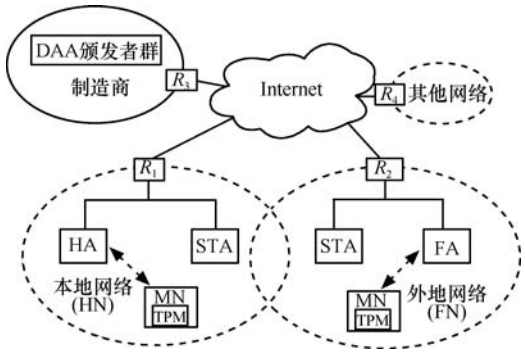

图 1 无线移动网络模型

4 可信的匿名无线认证协议

4.1 系统参数及符号定义

根据图 1 所构建的模型和文献[14]，给出本文相关参数和符号定义如表 1 所示。

表 1 符号定义

符号	定义
ID_{A}	实体 A 的身份
T_{A}	实体 A 产生的时戳
$Cert_{\mathrm{A}}$	实体 A 的证书
$(X)_K$	用密钥 K 对消息 X 进行对称加密
$E_K\{X\}$	用密钥 K 对消息 X 进行签名
$H(X)$	单向散列函数
KU_{A}	实体 A 的公钥
KR_{A}	实体 A 的私钥
n	Special RSA 模数
g	循环群 QR_n 的随机生成元
α, l_c, l_s, l_b	大于 1 的安全参数
Y	满足 $Y > 2^{\alpha(l_c+l_b)+1}$
X	满足 $X > 2Y + 2^{\alpha(l_s+l_c)+2}$
E, s	平台身份证书，满足 $E^s \equiv g \bmod n$
AIK_{pub}	平台 AIK 公钥
AIK_{priv}	平台 AIK 私钥
$\{X\}_{\mathrm{AIK}}$	AIK 签名运算
$\log(X)$	度量日志提取操作

4.2 协议描述

1) 第 1 阶段在本地网络注册。

当移动节点（MN）加入网络时，本地网络代理（HA）对其进行注册。在本方案中，HA 与 FA 的认证是通过有线网络进行的。假设在网络中有一个集中管理的 PKI 中心，HA 和 FA 都具有由 CA 签署的公钥证书，如 X.509 证书等。

合法的移动节点（MN）在 HA 处注册时，HA 首先完成对 MN 平台中 TPM 的身份验证。MN 利用 TPM 生成 AIK 密钥对 AIK_{priv} 和 AIK_{pub}，随后 MN 的平台主机及 TPM 产生随机数 $b \in_R [Y - 2^{l_b}, Y + 2^{l_b}]$，$t_1 \in_R \pm\{0,1\}^{\alpha(l_s+l_c)}$ 和 $t_2 \in_R \pm\{0,1\}^{\alpha(l_b+l_c)}$，计算 $T_1 = E^b \bmod n$，$T_2 = g^b \bmod n$，$d_1 = T_1^{t_1} \bmod n$，$d_2 = g^{t_2} \bmod n$，计算 $c = H(g \| T_1 \| T_2 \| d_1 \| d_2 \| AIK_{\mathrm{pub}})$，$w_1 = t_1 - c(s - X)$，$w_2 = t_2 - c(b - Y)$。接着，MN 发送消息 $(c, w_1, w_2, T_1, T_2, AIK_{\mathrm{pub}})$ 给 HA，同时该消息由 TPM 进行存储保护。收到消息后，HA 计算 $c' = H(g \| T_1 \| T_2 \| T_1^{w_1 - cX} T_2^c \| g^{w_2 - cY} T_2^c \| AIK_{\mathrm{pub}})$，接受此 TPM 来自合法的 DAA 颁发者，当且仅当 $c = c'$，$w_1 \in \pm\{0,1\}^{\alpha(l_s+l_c)+1}$，$w_2 \in \pm\{0,1\}^{\alpha(l_b+l_c)+1}$ 同时成立。

在确认 MN 的平台身份合法后，HA 给 MN 分配唯一的标识号 ID_{MN}，利用式(1)计算产生 MN 的临时身份 PID_{MN}，即

$$PID_{\mathrm{MN}} = H(ID_{\mathrm{MN}} \| N_m \| c) \oplus ID_{\mathrm{HA}} \oplus ID_{\mathrm{MN}} \quad (1)$$

其中，N_m 为 HA 随机选取的大数。HA 将 PID_{MN} 通过安全通道交给 MN，由 TPM 存储保护。HA 确定 MN 和 TPM 的绑定关系，并存储在数据库中。

2) 第 2 阶段在外地网络接入认证。

漫游至外地网络时，MN 通过外地网络代理 FA 接入网络，其接入认证过程如图 2 所示。

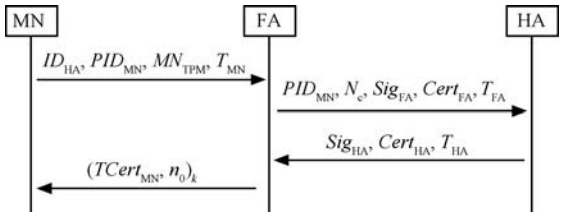

图 2 MN 在外地网络接入认证

其中，

$$MN_{\mathrm{TPM}} = (Q, Log, (c, w_1, w_w, T_1, T_2), AIK_{\mathrm{pub}}),$$

$$Sig_{\mathrm{FA}} = E_{KR_{\mathrm{FA}}}\{H(PID_{\mathrm{MN}}, N_c, Cert_{\mathrm{FA}}, T_{\mathrm{FA}})\},$$

$$Sig_{\mathrm{HA}} = E_{KR_{\mathrm{HA}}}\{H(Cert_{\mathrm{HA}}, T_{\mathrm{HA}})\}。$$

① 当 MN 进入新的外地网络，发送接入请求给 FA，开始 MN 与 FA 的认证。MN 利用 TPM 的随机数生成器产生一个秘密的随机数 x_0 并保存。MN 根据网络服务安全策略提取平台 PCR 值 PCR_{MN}，加载 AIK 私钥 AIK_{priv}，对 PCR_{MN} 进行 AIK 签名，即计算 $Q=\{PCR_{\mathrm{MN}},x_0\}_{AIK_{\mathrm{priv}}}$，导出 SML 日志 $Log=\log(SML)$，利用对 AIK_{pub} 的 DAA 签名消息等计算平台身份信息和完整性信息，即 $MN_{\mathrm{TPM}}=(Q,\ Log,(c,w_1,w_w,T_1,T_2),AIK_{\mathrm{pub}})$，同时，MN 产生时间戳 T_{MN}。最后，MN 发送消息 $ID_{\mathrm{HA}},PID_{\mathrm{MN}},MN_{\mathrm{TPM}},T_{\mathrm{MN}}$ 给 FA。

② FA 收到 MN 的访问请求后，检查其时戳的有效性，以此来防范重放攻击。如果无效，FA 拒绝 MN 的接入请求。随后，FA 对 MN 的平台身份和完整性进行验证。FA 计算 $c'=H(g\|T_1\|T_2\|T_1^{w_1-cX}T_2^{\,c}\|g^{w_2-cY}T_2^{\,c}\|AIK_{\mathrm{pub}})$，并判断 $c\overset{?}{=}c'$，$w_1\overset{?}{\in}\pm\{0,1\}^{\alpha(l_s+l_c)+1}$，$w_2\overset{?}{\in}\pm\{0,1\}^{\alpha(l_b+l_c)+1}$，如果均符合则平台身份合法，否则拒绝 MN 的访问请求。接着，FA 利用 MN_{TPM} 中的 AIK 公钥 AIK_{pub} 解密 Q 得到 PCR_{MN} 和 x_0，并验证其正确性，如果验证不通过，则 FA 拒绝 MN 的接入请求，否则进行下列操作。

FA 产生时戳 T_{FA}，计算 $N_c=H(c\oplus T_{\mathrm{FA}})$，用其私钥 KR_{FA} 对要发送的信息进行签名，即 $Sig_{\mathrm{FA}}=E_{KR_{\mathrm{FA}}}\{H(PID_{\mathrm{MN}},N_c,Cert_{\mathrm{FA}},T_{\mathrm{FA}})\}$。然后根据 MN 提供的 HA 的标识，发送 $PID_{\mathrm{MN}},N_c,Sig_{\mathrm{FA}},Cert_{\mathrm{FA}},T_{\mathrm{FA}}$ 给 HA。

③ HA 从 FA 处收到消息后，检查其证书和时戳是否有效。如果无效，则 HA 中止执行，否则 HA 按式(2)计算 MN 的身份标识，即

$$ID_{\mathrm{MN}}=PID_{\mathrm{MN}}\oplus H(ID_{\mathrm{MN}}\|N_m\|c)\oplus ID_{\mathrm{HA}} \quad (2)$$

得到 MN 的身份后，HA 进行验证，如果 MN 不是一个合法用户，HA 向 FA 发出“该用户非法”的消息。根据该身份对应的 c 值，HA 计算 $N_c'=H(c\oplus T_{\mathrm{FA}})$，并判断 $N_c'\overset{?}{=}N_c$，如果不相等，HA 向 FA 发出“该用户平台身份不合法”的消息，否则进行下列操作。

利用私钥 KR_{HA}，HA 对发送的消息进行签名，即 $Sig_{\mathrm{HA}}=E_{KR_{\mathrm{HA}}}\{H(Cert_{\mathrm{HA}},T_{\mathrm{HA}})\}$。HA 产生时戳 T_{HA}，然后将消息 $Sig_{\mathrm{HA}},Cert_{\mathrm{HA}},T_{\mathrm{HA}}$ 发送给 FA。

④ 从 HA 处收到消息，FA 确认了 MN 的身份合法性，随后检查其证书和时戳是否有效，如果无效，则中止执行，否则 FA 确认 MN 为 HA 的使用平台可信的合法注册用户。FA 签发临时证书 $TCert_{\mathrm{MN}}$ 给 MN，包含证书有效期限等相关信息。随后，FA 产生随机数 n_0，计算密钥 $k=x_0$ 并保存，利用 k 对临时证书 $TCert_{\mathrm{MN}}$ 和 n_0 进行加密，将消息 $(TCert_{\mathrm{MN}},n_0)_k$ 发送给 MN。

从 FA 处收到消息后，MN 对 $(TCert_{\mathrm{MN}},n_0)_k$ 进行解密得到临时证书 $TCert_{\mathrm{MN}}$ 和随机数 n_0 并保存。

3) 第 3 阶段在外地网络进行访问。

在临时证书 $TCert_{\mathrm{MN}}$ 的有效期内，当 MN 对 FA 进行第 i 次访问时，其过程如图 3 所示。

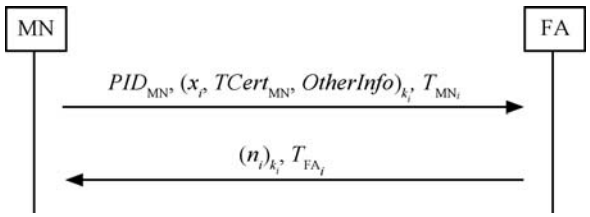

图 3　MN 访问外地网络

① MN 利用 TPM 产生随机数 x_i，利用式(3)计算本轮临时身份 PID_{MN_i}，即

$$PID_{\mathrm{MN}_i}=PID_{\mathrm{MN}_{i-1}}\oplus n_{i-1}$$

$$PID_{\mathrm{MN}_0}=PID_{\mathrm{MN}},i=1,2,3,\cdots,n \quad (3)$$

利用式(4)计算本轮会话密钥 k_i，即

$$k_i=x_{i-1}\oplus n_{i-1},k_0=k,i=1,2,\cdots,n \quad (4)$$

用 k_i 对要发送的部分消息进行加密，即计算 $(x_i,TCert_{\mathrm{MN}},OtherInfo)_{k_i}$。随后，MN 产生时戳 T_{MN_i}，发送消息 $PID_{\mathrm{MN}_i},(x_i,TCert_{\mathrm{MN}},OtherInfo)_{k_i},T_{\mathrm{MN}_i}$ 给 FA。

② FA 收到消息后，首先利用式(3)验证 MN 的身份 PID_{MN_i}，即计算 $PID_{\mathrm{MN}_i}=PID_{\mathrm{MN}_{i-1}}\oplus n_{i-1}$，检查临时证书 $TCert_{\mathrm{MN}}$ 和时戳 T_{MN_i} 是否有效，如果无效，则拒绝 MN 的访问请求，否则，FA 利用式(4)计算 k_i，然后解密得到 $x_i,TCert_{\mathrm{MN}},OtherInfo$，并比较解密得到的证书与原颁发证书的一致性，若一致则进行如下操作。FA 将 x_i 保存，用来计算下一次的会话密钥。FA 产生新的秘密随机数 n_i，并生成新的时戳 T_{FA_i}，发送消息 $(n_i)_{k_i},T_{\mathrm{FA}_i}$ 给 HA。其中，$OtherInfo$ 可以是 MN 的平台信息，根据需要 FA 可再次验证 MN 的平台身份和完整性以确认其可信性。

5 协议分析

5.1 安全性分析

1) 方案安全性。

方案中，HA 与 FA 的认证使用公钥证书，其安全性得到保证。MN 在本地网络注册时，注册信息的请求和发送通过安全通道进行，难于受到攻击者的窃听和篡改，其安全性得到保证。

当 MN 在外地网络访问时，为了验证 MN 的合法性，FA 将 MN 发来的信息转发给本地网络代理 HA，同时对主要消息进行散列运算，保证消息的完整性，并通过时戳和随机数来防止重放攻击。HA 验证 FA 的合法性后，通过式(2)计算得到 MN 的身份，即可验证 MN 的合法性。在发送给 FA 的消息中，HA 同样采用了时戳和随机数来保证其新鲜性并可防止重放攻击。

在临时证书的有效期内，MN 访问外地网络时，使用临时证书 $TCert_{\mathrm{MN}}$ 证明自己的合法身份，且每次均产生不同的会话密钥，实现了一次一密，具有前向保密性。在 MN 与 FA 的认证过程中，x_i 由 MN 利用 TPM 选择产生，n_i 由 FA 选择产生，见式(4)。因此，在对 FA 的访问中密钥 k_i 被作为一次性密钥使用，具有强的新鲜性，且任何一方不能单独产生 k_i，保证了会话密钥的公正性。另外，随机数 x_i 产生自 TPM 内部，其安全性得到增强。

2) 平台身份匿名性和不可伪造性。

定义 1 DDH 假设（decisional Diffie-Hellman assumption）

设 k 为安全参数，p,q 为素数，其中 q 的长度为 k 比特，且 $q \mid p-1$，g 是阶为 q 的群 Z_p^* 中元素，x,y,z 是从 Z_p 中均匀选择的，则对于任何的多项式时间算法，$Q_0=\{< p,g,g^x,g^y,g^{xy} >: x,y \leftarrow^R Z_p\}$ 与 $Q_1=\{< p,g,g^x,g^y,g^z >: x,y \leftarrow^R Z_p\}$ 的概率分布是计算不可区分的。

定理 1[14] 在 DDH 假设下，DAA-ED 方案能够完成 TPM 身份对验证者的匿名证明。

根据定理 1，在本方案中，移动节点 MN 的平台身份对于 HA 和 FA 是匿名的，HA 和 FA 均能验证该平台中的 TPM 来自正确的颁发者群，而不能确定其具体身份。因此，方案中移动节点 MN 的平台身份满足匿名性。

定义 2 强 RSA 假设（strong RSA assumption）

设 n 是 RSA 模数，$z \in Z_n^*$ 是随机元素，Flexible RSA 问题是指找到 $e>1$ 和 $u \in Z_n^*$，使其满足 $u^e \equiv z \bmod n$。强 RSA 假设是指不存在多项式时间算法能够以不可忽略的概率解决 flexible RSA 问题。

定理 2 在强 RSA 假设下，移动节点 MN 的平台身份和完整性信息不能被伪造。

证明 首先，基于强 RSA 假设，攻击者通过直接猜测或者在已获知多个合法证书密钥对 $(E_1,s_1),(E_2,s_2),\cdots,(E_r,s_r)$ 的基础上均不能完成对 TPM 的 AIK 公钥 AIK_{pub} 的 DAA 签名，平台身份具有不可伪造性[14]。

其次，对于平台完整性信息 PCR_{MN}，TPM 进行实时的 AIK 签名。一方面，攻击者不掌握 AIK 私钥 AIK_{priv}，无法完成对平台完整性信息的 AIK 签名。另一方面，根据定理 1，TPM 对 AIK 公钥 AIK_{pub} 的 DAA 签名也不能被伪造。因此，平台完整性信息也不能被伪造。

所以，攻击者通过直接猜测或者在已知多对合法证书密钥对基础上，既不能对新的合法 TPM 身份签名信息进行伪造，也不能对平台完整性信息进行伪造，方案中 MN 的平台身份及完整性信息具有不可伪造性。

3) 用户身份匿名性和不可跟踪性。

方案参与方的所有交换消息中均未使用 MN 的真实身份，在本地网络注册时用户真实身份 ID_{MN} 被临时身份 ID_{MN} 替代，见式(1)。只有掌握秘密数 N_m 和知晓平台 DAA 签名消息 c，才能利用式(2)计算得到 MN 的真实身份 ID_{MN}，而只有本地网络代理 HA 知晓秘密数 N_m 并能够与正确的 c 值对应，因此，只有 HA 能通过式(2)正确验证 MN 的真实身份 ID_{MN}，确保了用户身份的匿名性。跟踪者未获知该秘密值，不能通过方案中交换的消息得到用户的真实身份或者确定用户的位置。

不同的 ID_{MN} 与不同的移动用户相对应，且使用互不相同的随机数 N_m 和签名信息 c 计算产生。任何合法的移动用户均不能通过 ID_{MN} 计算得到其他合法用户 MN 的身份信息 ID_{MN}，从而无法假扮其他用户，可有效地克服针对用户匿名性的攻击。用户多次访问外地网络时，每次均使用不同的临时身份 PID_{MN_i}，同样具有不可跟踪性。假设某种原因，MN 的身份 ID_{MN} 被泄漏，由于 HA 和 FA 同时验证用户的临时身份、平台信息及对应关系，并且根据定理 2，

用户平台信息不能被伪造，可再次保证不被假冒。

用户每次接入外地网络时使用不同的临时身份，且会话密钥每次均不同，具有强的一次一密性。当用户接入不同的外地网络时，所使用的临时身份和会话密钥也不同，可有效防止网络代理或非法用户利用历史数据对用户的跟踪，满足域分离特性。

4) 平台可信性验证。

在本地网络完成注册并进行访问时，MN 可根据需要通过向 HA 提供经过 AIK 签名的平台 PCR 值及度量存储日志 SML，以证明平台的完整性。平台信息是 TPM 从硬件开始获取的移动终端平台的各种配置信息，并由底层传递至应用层，是从可信根通过信任链进行传递的过程，从而 HA 确定 MN 是可信的。

当用户漫游至外地网络进行接入访问时，由于 MN 的平台从外地网络获取服务，如果其系统存在安全缺陷，会对外地网络造成安全危害。因此，采用直接匿名证明方案，由 FA 直接验证 MN 的身份正确性和平台可信性更为安全有效。当 MN 在临时证书的有效期内多次访问时，FA 可根据安全策略对 MN 提出完整性验证的要求，保证 MN 平台可信性再次被验证。

5.2 性能分析

1）安全性能分析。

本方案与其他无线接入认证方案在能够达到的安全性能方面进行对比分析，其结果如表 2 所示。其中，“Y”表示达到或满足，“N”表示未达到或不满足，“—”表示不涉及该功能。

表 2　　安全性能比较

安全功能	Zhu[4]	Peng[5]	Yang[11]	本方案
用户匿名	Y	Y	Y	Y
域分离性	N	Y	Y	Y
双向认证	Y	Y	Y	Y
一次性密钥	Y	Y	Y	Y
密钥协商公正性	N	N	Y	Y
平台直接匿名	—	—	N	Y
平台可信验证	—	—	Y	Y

从表 2 中的数据可以看出，与传统的无线匿名认证方案（文献[4]和文献[5]）相比，本方案在达到基本安全目标如用户匿名、双向认证等的基础上，增加了对移动终端平台的可信性验证，增强了方案的安全性能和对攻击的抵抗能力，能够更好地保障无线认证系统中终端用户免受恶意攻击者的侵害，并大大减少认证代理服务器所受到的不满足安全策略的移动终端的安全威胁。与文献[11]的方案相比，当 MN 漫游至外地网络时，由外地网络服务器提供服务，MN 的平台身份和可信性由 FA 直接验证将更加安全有效，更符合漫游业务的需求。因此，与已有方案相比较，本方案能够达到更多的安全目标和更好的安全性。

2) 计算性能分析。

无线移动网络中移动终端的计算能力有限，协议的效率主要用协议执行过程中移动终端所完成的各种计算来衡量。将本文方案与已有方案的运算量进行分析对比，其结果如表 3 所示，分析时仅考虑移动终端的计算代价。其中，“XR”表示异或运算，“H”表示散列运算，“EX”表示模指数运算，“EK”表示对称加密运算，“DK”表示对称解密运算，“TS”表示 TPM 的 AIK 签名运算。

表 3　　计算性能比较

方案名称	主机 CPU 计算量	TPM 计算量
Zhu[4]	4XR+2H+2EK+2DK	—
Peng[5]	4XR+1H+2EX+1DK	—
Yang[11]	3XR+1H+2EK+1DK	2H+2TS
本方案	2XR+2EK+1DK	2H+2TS

分析中，将移动终端平台 CPU 的计算量与 TPM 的计算量分别计算，对于平台 CPU，与文献[4]方案和文献[5]方案相比，协议执行了 2 次异或运算、2 次对称加密运算和 1 次对称解密运算，计算量相对较小，不对移动平台造成影响。TPM 芯片作为独立的计算单元，可以加速方案的执行，2 次签名运算和 2 次散列运算都由 TPM 完成，不消耗平台主机 CPU 的计算性能。假设文献[4]方案和文献[5]方案中也增加可信验证功能，那么其协议中至少增加 2 次 AIK 签名运算和 2 次散列运算，平台总的计算量仍然比本方案复杂。与文献[11]的方案比较，对于平台主机 CPU 减少了 1 次散列运算，对于平台 TPM，计算量基本相同，但平台身份信息和完整性信息由 FA 直接验证，无需转发给 HA，减少了方案的通信量。

方案中，移动终端向 FA 发送平台完整性信息，增加了一定的消息负载。根据安全策略的不同发送 PCR 值，每个 PCR 值长度为 160bit，TPM 对于 AIK 公钥的 DAA 签名经过散列运算后消息长度固定，SML 依据所计算的 PCR 来决定，平台完整性信息的消息长度在可接受的范围内。但是，所增加的消息负载提供了平台可信验证，且方案的部分参数可以通过预计算得到，移动终端平台 CPU 与 TPM 可

以同时完成部分运算，一定程度地缩短运算时间，减少通信时延。综合来看，本方案具有更高的效率，满足可信计算环境下移动终端的漫游业务的需求。

6 结束语

本文提出可信计算环境下直接匿名的无线网络接入认证方案，利用远程证明方法由外地网络代理服务器直接验证平台身份和完整性，借助本地网络代理服务器验证用户身份，方案安全高效具有匿名性、可信验证性、域分离性等特点，满足无线移动网络需求。但本方案采用二进制方法[6]完成平台完整性的校验，由于 FA 对 MN 的平台可信性进行直接验证，可能会暴露平台部分配置信息。因此，本文进一步的工作将结合属性证明[16]等来完成平台完整性的校验，以更好地保护平台配置信息的隐私性。

参考文献：

[1] Third Generation Partnership Project (3GPP), Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 8), 3GPP TS 33.821 v1.0.0[S]. 2007.

[2] CAIMU T, OLIVER W. Mobile privacy in wireless networks- revisited[J]. IEEE Transactions on Wireless Communications, 2008,7(3): 1035-1042.

[3] PARK C S. Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems[J]. Computer Networks, 2004,44(2): 267-273.

[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 J M, MA J F. An efficient authentication protocol with anonymity for wireless IP networks[J]. Journal on Communications, 2004, 25(6):12-18.

[5] 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 H X, FENG D G. Security flaws and improvement to a wireless authentication protocol with anonymity[J]. Journal on Communications, 2006, 27(9):78-85.

[6] Trusted Computing Group. TCG specification architecture overview[EB/OL]. http://www. trustedcomputinggroup.org, 2007.

[7] 沈昌祥, 张焕国, 冯登国等. 信息安全综述[J]. 中国科学 E 辑. 2007,37(2):129-150.
SHEN C X, ZHANG H G, FENG D G, *et al*. Survey of information security[J]. Science in China(Information Sciences), 2007,37(2): 129-150.

[8] 张焕国, 罗捷, 金刚等. 可信计算研究进展[J]. 武汉大学学报(理学版), 2006, 52(5): 513-518.
ZHANG H G, LUO J, JIN G, *et al*. Development of trusted computing research[J]. Journal of Wuhan University (Natural Science Edition), 2006, 52(5):513-518.

[9] 郑宇, 何大可, 何明星. 基于可信计算的移动终端用户认证方案[J]. 计算机学报，2006, 29(8):1255-1264.
ZHENG Y, HE D K, HE M X. Trusted computing based user authentication for mobile equipment[J]. Chinese Journal of Computers, 2006,29(8):1255-1264.

[10] Trusted Computing Group. Trusted computing platform alliance (TCPA) main specification[EB/OL]. http://www.trustedcomputing-group. org, 2001.

[11] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. 通信学报，2009, 30(9):29-35.
YANG L, MA J F, ZHU J M. Trusted and anonymous authentication scheme for wireless networks[J]. Journal on Communications, 2009, 30(9):29-35.

[12] BRICKELL E, CAMENISCH J, CHEN L Q. Direct anonymous attestation[A]. Proceedings of the 11th ACM Conference on Computer and Communications Security[C]. New York, NY, USA, 2004. 132-145.

[13] CAMENISCH J, LYSYANSKAYA A. Dynamic accumulators and application to efficient revocation of anonymous credentials[A]. Cryptology - CRYPTO 2002[C]. Springer Verlag, 2002.61-76.

[14] GE H, TATE S R. A direct anonymous attestation scheme for embedded devices[A]. PKC 2007[C]. Springer, Heidelberg,2007.

[15] CAMENISCH J, MICHELS M. A Group Signature Scheme Based on an RSA-Variants[R]. Technical Report RS-98-27, BRICS, University of Aarhus, 1998.

[16] SADEGHI A, STUBLE C. Property based attestation for computing platforms: caring about properties, not mechanisms[A]. Proceedings of New Security Paradigms Workshop[C]. New York, 2004.67-77.

作者简介：

杨力（1977-），男，陕西乾县人，西安电子科技大学博士生、讲师，主要研究方向为可信计算、网络安全等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全、密码学等。

裴庆祺（1975-），男，广西桂林人，博士，西安电子科技大学副教授，主要研究方向为信息安全、内容保护等。

马卓（1980-），男，陕西延安人，西安电子科技大学博士生，主要研究方向为密码学、可信计算等。