doi:10.3969/j.issn.1000-436x.2012.z1.004

基于云计算的智能手机社交认证系统

刘宴兵，刘飞飞
（重庆邮电大学 计算机科学与技术学院，重庆 400065）

摘 要：云计算提供无限存储和计算的能力可以弥补移动终端资源受限的缺陷。因此针对已提出的社交认证方法对认证票据的有效期需求时间长且终端资源消耗量大的问题，设计了一种基于云计算的智能手机社交认证系统。该系统综合考虑 3 种社交网络特性：各好友不同的认证权威性、个体的行为差异性和每次交互事件所携带的信任度。通过实验验证，本认证系统在降低终端能耗和增强身份认证安全性的情况下有效地解决了认证票据有效期短而导致系统性能急剧下降的问题。

关键词：云计算；智能手机；社交认证
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0028-07

Cloud computing based smartphone social authentication system

LIU Yan-bing, LIU Fei-fei
(School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Cloud computation provided the capabilities to store and compute infinitely, which can filled the gap of resource constrain. So a cloud-computation based social authentication system for smartphones aimed at the problem that the present authentication methods require a long period of validity of the authentication tokens and make the terminals consume large resources was proposed. The system took three types of social networking features into considered, which were different certification authority between the friends, behavior differences between individual and trust level carried by each interactive event. The results of experiments show that the system can effectively solve the problem that system performance will sharply decline when the expiry date of authentication tokens is short.

Key words: cloud computing; smartphone; social authentication

1 引言

云计算和移动互联网是当前信息领域的研究热点。随着云计算的发展，云服务数量和种类爆炸式增长。各种云服务极大地提高了用户体验，同时越来越多的人们通过手机等移动终端接入网络和云服务，但对于银行账号、个人资料、公司数据等私密信息的接入必须进行安全审查。传统的认证方式主要通过账号/密码实现，其安全性受到密码复杂性的影响。但由于手机输入方式的限制，当安全性与方便性发生冲突时，人们更倾向于选择方便性(即简单的密码)[1]。因此移动终端和云服务提供商对于既安全又方便的认证机制的需求更加迫切。另一方面，由于手机端在计算、存储和电池等方面存在资

收稿日期：2012-08-06
基金项目：“新一代宽带无线移动通信网”国家科技重大专项课题基金资助项目（2011ZX03002-004-03）；国家自然科学基金资助项目（61272400）；教育部 NCET；重庆市高校成果转化项目（Kjzh10206）；公安部信息网络安全重点实验室项目（C11609）
Foundation Items: “The Next-Generation Broadband Wireless Mobile Communication Network” National Science and Technology Major Project (2011ZX03002-004-03); The National Natural Science Foundation of China (61272400); NCET； R&D Foundation of Chongqing Municipal(Kjzh10206); Open Project of Key Lab of Information Network Security of Administration of Public Security (C11609)

源受限的特点，使得 PC 上传统的身份认证方式并不完全适合移动终端。由于云计算的特点是为用户提供无限的存储、计算等 IT 服务，因此云计算恰好可以弥补移动终端资源受限的缺陷。

因为云计算和移动终端具有不同的特性，目前对于手机身份认证方式的研究主要从用户行为、社交网络和生物特征 3 个方面提取认证用户身份的信息及利用云计算弥补终端资源受限的缺陷。Mauro Conti 等提出了基于用户接电话动作的移动终端认证方式[2]，将用户点击接听键至开始通话的间隔时间作为识别用户依据。J. Guerra-Casanova 等提出了根据用户拿手机时的姿态作为识别用户身份的依据[3]。P.A.Tresadern 等给出了通过手机实时跟踪脸部的方法[4]，达到识别用户身份的目的。Richard Chow 等提出了一种云环境中基于用户行为的移动终端认证框架[5]，其中考虑了终端的资源受限特性，将大部分计算任务转移到云服务器中。RSA 实验室最先提出了社交认证的概念，通过电话向合法用户申请认证码后，使用认证码作为依据进行身份认证[6]。Stuart Schechter 等提出了一种基于社交网络特征的备用认证方式，用于代替流行的基于 E-mail 的备用认证方式[7]。Soleymani B 等提出了一种基于社交网络分析的智能手机认证协议 (SAP, social authentication protocol for mobile phones)[8]，通过将用户的通信网络看作社交网络，从社交网络角度提出一种手机的认证协议。但是其提出的认证协议并未考虑移动终端的资源受限特性。

因此本文提出了基于云计算的智能手机社交认证系统。利用多种手机网络中存在的社交特性，并将大量的存储和计算任务放在云端进行，减少了对终端的资源消耗，从而保证了认证成功率，增强了身份认证的安全性并提高了终端用户的使用体验。

2　基于云计算的智能手机社交认证系统设计

身份认证的目的是一方向另一方证明自己就是所声称的合法用户，即让另一方信任自己的合法身份[9]。然而信任是可以被传递的，在电子商务的实际应用中通过传递信任来降低交易风险[10]。本文提出的基于云计算的智能手机社交认证系统将好友与用户间符合一定要求的通信行为（如通话、短信、蓝牙及红外的接入等）看作是两者之间相互信任的表现，并将这种信任传递给认证中心，认证中心根据收到用户被好友信任的情况决定是否信任用户，即是否认可用户身份的合法性，通过信任的传递来实现身份认证功能。

本论文设计的认证系统由 3 部分组成：1) 用户手机端；2) 认证中心；3) 应用服务器。手机端分为用户和好友 2 种角色，手机端由权重计算模块、认证票据生成模块、数据安全管理模块、数据通信模块组成。认证中心由 PKI 服务器、认证服务器及数据库组成。基于云计算的智能手机社交认证系统结构如图 1 所示。

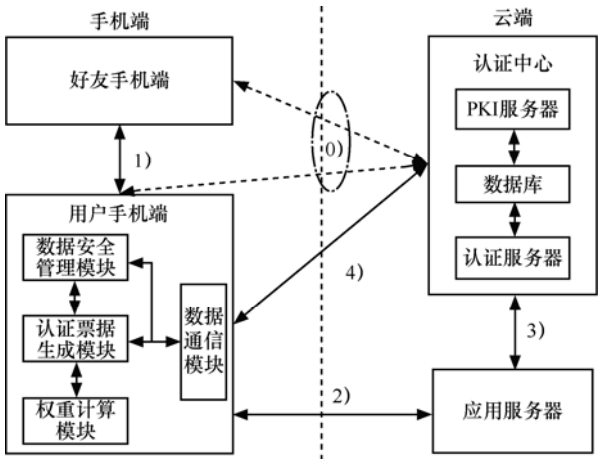

图 1　身份认证系统结构

系统运行分为以下 3 个过程。

1) 系统初始化过程

用户手机请求在认证中心登记注册，通过 PKI 服务获得公钥/私钥和提交好友列表；认证中心通知手机联系人建立好友请求。当用户和联系人间建立好友关系后，用户通过 PKI 服务获得好友最新的公钥，同样好友通过 PKI 获得用户最新的公钥。

2) 分发认证票据过程（信任分发）

用户及好友的手机端权重计算模块根据用户的通信行为（如通话、短信、蓝牙及红外的接入等信息）判断是否达到信任要求（即是否信任对方）并计算出认证权重。认证票据生成模块通过信息安全管理模块获得密钥，通过权重计算模块获得认证权重后，生成信任的载体——认证票据。

用户及好友的手机端通过数据通信模块发送、接收认证票据，用户及好友的手机端将接收到的认证票据交于数据安全管理模块。

3) 身份认证过程（信任传递）

用户使用手机接入网络中需要身份认证的服务时，提供服务的应用服务器将身份认证工作转交给认证中心；当认证中心收到网络中应用服务器的

身份认证请求后，通知用户手机进行身份认证；用户手机响应认证请求，通过认证票据与密钥安全管理模块及数据通信模块，发送收集到的全部认证票据到认证服务器；认证中心根据收到的认证票据及发放票据的各好友对应的影响因子计算出有效权重值后（认证中心通过传递获得的信任），与认证服务器中设定认证门限值做比较获得认证结果。将结果返回给应用服务器。，当认证失败时要求用户通过账号/密码方式强行认证。

通过以上步骤，可以使认证中心相信用户的好友是否认可用户身份的合法性。通过累计这样的信任获得对用户身份的信任度，最终达到认证用户身份的目的。本身份认证系统的认证过程对于用户是透明的，只有在认证失败的时候才需要用户的参与，极大地方便手机用户的使用。

手机端需要保存的数据有：好友的公钥、自己的私钥、收集到的认证票据和少量的通信行为记录。需要的计算的任务有：判断通信行为是否达到可信要求、生成认证票据、发送和接收信息。

云端需要保存的数据有：认证中心自己的私钥、系统中用户的全部公钥、全部用户的通信行为记录、各用户的不同认证门限值、各用户好友按熟悉度的排列顺序等。需要进行的计算任务有：计算用户好友的排名、计算用户每次认证时的有效认证值、计算用户的认证门限值、系统中全部密钥的管理等。云端需要存储海量的数据及进行繁重的计算任务。

由于认证协议保证了身份认证的安全性和高效性，所以认证协议是本系统的核心部分。下一节详细阐述本认证系统所使用的认证协议。

3 多种社交特征的认证协议(VSAP, validity of the social features authentication protocol)

3.1 认证协议设计

本文设计的多种社交特征的认证协议（VSAP）充分考虑了手机通话网络中的社交网络特性。针对用户的不同好友影响权重不同的特性分别给予好友不同的影响因子，使得越熟悉的好友其认证的权威性越高。由于交互事件本身携带大量信任信息，量化信任信息可以体现各交互事件的可信度，使得在认证过程中可信度越高的交互事件获得的认证权重越高。考虑到用户个体行为的差异性，各用户所能获得的权重值的范围不同，故在设定认证门限时，对不同的用户设定不同的认证门限，提高认证的安全性和准确性。多种社交特征的认证协议各符号意义如表1所示。

表1 认证协议中符号意义

符号	语义
A	用户标识符
B	好友标识符
S	认证中心标识符
T_{valid}	票据的有效期
T_{ba}	时间戳
I_{ba}	认证权重
R_{Ab}	好友B对用户A的影响因子
K_{Ss}	认证中心的私钥
K_{Sx}	用户X的私钥
K_{Px}	用户X的公钥
K_{Ps}	认证中心的公钥

VSAP的消息流程如下。

1) 当用户A与好友B通信行为达到信任门限时，B使用自己的私钥生成认证票据$\{A, I_{ba}, T_{\text{valid}}\}K_{Sb}$，并添加时间戳$T_{ba}$，最后用$A$的公钥加密整个信息后发送给$A$，消息为$\{\{A, I_{ba}, T_{\text{valid}}\}\ K_{Sb}, T_{ba}\}K_{Pa}$。

2) A接收到B发来的消息后使用自己的私钥K_{Sa}解密消息。当验证T_{ba}有效时，则保存证明票据$\{A, I_{ba}, T_{\text{valid}}\}K_{Sb}$。否则将此票据丢弃。

3) 当A需要进行身份认证的时候，A取出收集到的所有认证票据，添加时间戳和自己的身份标识A，最后用S的公钥K_{Ps}加密后发送给中心认证服务器S，消息为$\{\{A, I_{ba}, T_{\text{valid}}\}K_{Sb}, T_{as}, A\}K_{Ps}$。

4) S接收到认证消息后使用私钥K_{Ss}解密消息，当验证T_{as}有效时，解密认证票据$\{A, I_{ba}, T_{\text{valid}}\}K_{Sb}$。由于只有使用$B$的公钥$K_{Pb}$才能解密，所以当解密成功后，认证服务器可确信此张认证票据是好友B发送给A的，认证服务器就可以获得好友B对用户A的影响因子R_{Ab}。然后比较获得的2个A值，当2个A值相同时，进一步验证T_{valid}的有效性，否则认证失败。当T_{valid}有效时，A的一张认证票据中的I_{ba}有效，并使用$R_{Ab} \cdot I_{ba}$获得最终有效认证权重值，否则此张票据失效。类似计算其他的认证票据，当累计有效的认证权重值达到认证门限时，则认定A的身份认证成功，否则为认证失败。认证服务器根据认证结果确定下一步操作。

手机端的数据安全管理模块定时检查所保存

的认证票据的有效期，删除过期的认证票据。其中手机端定时上传通信行为记录到认证中心，认证中心根据用户的通信记录计算出用户各好友的影响因子。认证中心根据用户获得的有效权重值的范围计算出各用户的认证门限。

3.2　认证协议安全性分析

对于 VSAP 的攻击行为分为攻击者不能接触手机和攻击者可以接触手机 2 种情况。在攻击者可以接触手机时又分为手机中存有足够的认证票据和没有认证票据。分别讨论这几种常见的攻击方式对本认证协议的影响。

3.2.1　攻击者不接触手机

在此情况下，攻击者要达到成功认证的目的，必须要获得足够多的认证票据。当攻击者通过监听等手段获得好友认证消息 $\{\{A,I_{ba},T_{\text{valid}}\}K_{Sb},T_{ba}\}K_{Pa}$ 时，要获得认证票据 $\{A,I_{ba},T_{\text{valid}}\}K_{Sb}$，则必须使用用户 A 的私钥 K_{Sa} 解密消息。当攻击者获得了用户 A 的私钥后，则可以生成用户与认证中心间的认证消息 $\{\{A,I_{ba},T_{valid}\}K_{Sb},T_{as},A\}K_{Ps}$。因此在攻击者不能接触手机的情况下，身份认证的安全性依赖于用户 A 私钥的安全性。

3.2.2　攻击者占有手机

为了方便手机用户的使用，安全认证过程一般在后台自动完成，无需用户的介入，所以其密钥必须存储在手机中。由于手机的便捷性、易失性使得其硬件资源相对于 PC 更容易被攻击者接触到。当攻击者获得用户 A 的手机时，将可以得到 A 的私钥。根据之前分析，则身份认证的安全性将得不到保证，即攻击者可以从好友认证消息中获得认证票据 $\{A,I_{ba},T_{\text{valid}}\}K_{Sb}$ 以及生成服务器认证消息 $\{\{A,I_{ba},T_{\text{valid}}\}K_{Sb},T_{as},A\}K_{Ps}$。由此看来攻击者将能够成功冒充 A 获得系统的认证。但是这存在前提假设：手机中必须存在足够多的有效认证票据 $\{A,I_{ba},T_{\text{valid}}\}K_{Sb}$。下面按攻击者获得手机时，手机中认证票据的不同情况分别讨论。

1) 手机中没有认证票据

攻击者现在最需要的是获得足够多认证票据，而认证票据是由用户 A 的好友按照系统的规则产生，攻击者并不能操控好友的行为。所以攻击者只能试图去模仿用户 A 与好友联系。但是这样的操作是相当困难的。例如通话时长规则，攻击者在冒充 A 时，是很容易被 A 的好友发现。另一方面，冒充者并不了解用户 A 指定了哪些联系人为好友，也增加了其获得认证票据的难度。

2) 手机中存在足够多的认证票据

在这种情况下，攻击者可以通过获得的密钥和认证票据完成身份认证过程。但是只能在票据的有效期内完成。VSAP 的安全性还依赖于手机中认证票据的更新频率，认证票据有效期越短则其安全性越高。

4　信任度、好友影响因子、认证门限的选择

本论文中主要以通话形式的交互事件作为社交行为进行分析，并给出系统中信任度、好友影响因子及认证门限的一种计算方式。

定义 1　用户认证门限占其获得的有效认证值比例（PATA, proportion of authentication threshold occupies authentication weight）。PATA 表示系统在认证时所使用到的有效认证值占用户所获得的全部有效认证值的比例。PATA 越高表示在身份认证时用户所获得的有效认证值的利用率越高，可以有效地抵御假冒攻击，使得系统认证安全性更高。相反，PATA 越低，表示系统认证时浪费用户获得的有效认证票据数越多，认证的安全性越低。

4.1　信任度

本系统采用当用户与好友间通话时间超过判定门限则认为两者就是相互信任的，并根据通话时间量化信任度。认为通话时间越长，则互相信任度越高。采用的通信行为信任度即认证权重的计算函数为

$$\varpi(x)=\exp\left(a\left(\frac{x}{60}-\theta\right)\right)-1,\ \left(\frac{x}{60}>\theta\right) \tag{1}$$

其中，$\varpi(x)$ 为认证权重，x 为通话时间，单位为 s，a 为调节系数，本文中取 a=0.1；θ 为通信行为判断门限，当通话时间低于 θ 时，认为双方不构成相互信任关系，θ 越高表示对可信行为的要求越高，即将更多可信度低的交互事件判定为不可信，可以保证认证的安全性。如图 2 和图 3 所示，随着 θ 值的增加，用户达到门限的交互事件数量不断减少，由于没有足够的可信事件发生，使系统中可以传递的信任度减少，从而导致系统认证成功人数不断下降。另一方面，如图 4 所示，PATA 随着 θ 值的增加而下降，表示在相同的条件下用户获得的认证票据数量越多，身份认证时利用的票据数量越多，身份认证则越安全。所以选择 θ 值时，应当考虑到对 PATA 的影响。本文选取 θ=10(min)。

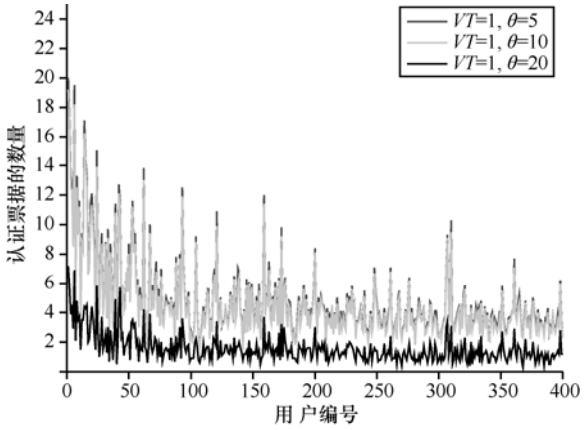

图 2　用户获得的认证票据数量（VT:认证票据有效期）

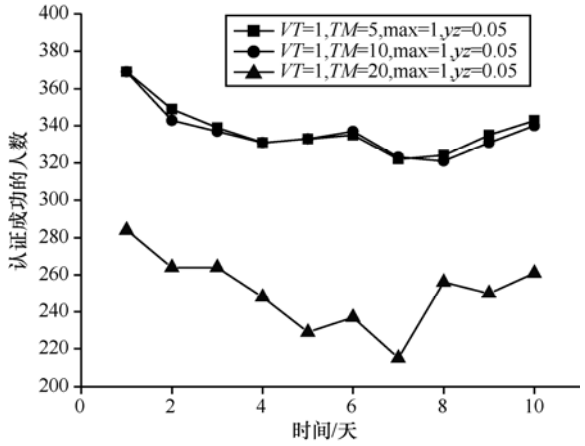

图 3　系统认证成功人数（VT:认证票据有效期）

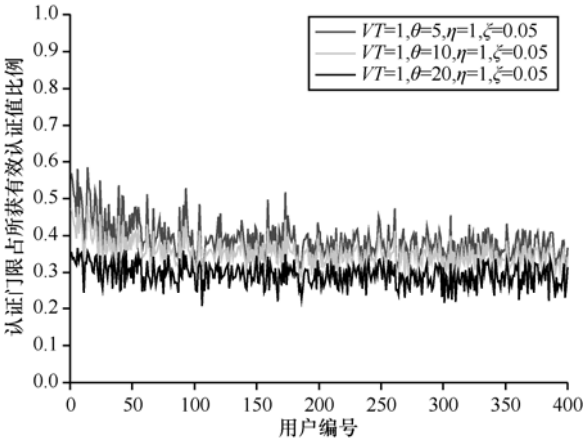

图 4　用户认证门限占其获得的有效认证值比例（VT:认证票据有效期）

4.2　好友影响因子

由于各好友与用户是熟悉度不同的，所以各好友的认证权威也应是不一样的。因此本协议中按与好友的熟悉度给各好友分配不同的影响因子。本文仅考虑通话信息这一维度，好友的熟悉度由使用好友与用户间的通话总时间作为依据并按降序排序，本文采用的好友影响因子计算式为

$$R_{Ax} = \eta - \kappa_x \xi \tag{2}$$

其中，R_{Ax} 为用户 A 的好友 x 的影响因子，κ_x 为好友 x 在用户 A 好友中的熟悉度排名，η 为调整系数，使得 R_{Ax} 大于 0。当 η 和 ξ 的联合变化时，对用户获得的认证票据的数量及每张票据中的信任度无影响，只影响用户获得有效认证值的大小。下面利用 R_{Ax} 值的变化，分析用户认证门限计算方式的特性。

由图 5 和图 6 可知，R_{Ax} 越大则户获得的有效认证值越大，使得 PATA 越高，但认证成功率越低。可以看出本文给出的认证门限计算方式具有使获得有效认证值越高用户的 PATA 越高的特点。同时，PATA 越高，则认证成功率越低。本文实验中取 η=2，ξ=0.1。

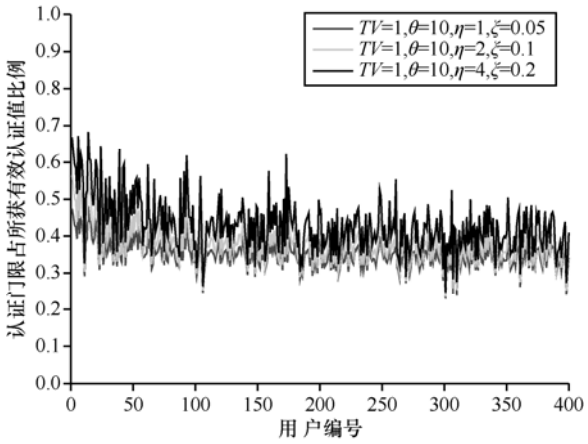

图 5　用户认证门限占其获得的有效认证值比例（VT:认证票据有效期）

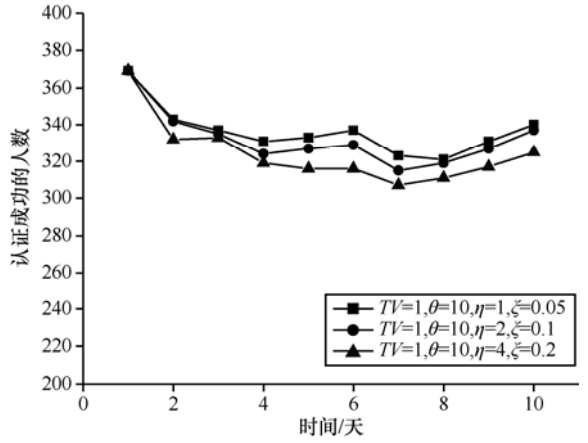

图 6　系统认证成功人数（VT:认证票据有效期）

4.3　用户认证门限

由于个人行为的差异性，导致用户所获得的权重值的范围不同，所以在设定认证门限时需考虑个体的差异性。本文提出了针对不同用户设定不同认证门限的方式来提高认证协议的可用性和安全性。

对不同的用户设定认证门限值应当达到以下要求：1) 获得的认证权重值波动大的用户认证门限低。（提高认证的成功率）；2) 获得的认证权重值高的用户认证门限高（提高认证的安全性）；3) 认证门限值不应高于用户成功认证时获得认证权重的均值。本文采用的用户认证门限计算函数为

$$f_i(x)=\frac{ave}{1+\left(\frac{\pi}{2}-\arctan\left(\frac{ave}{\beta}\right)\right)+\frac{var}{ave}},\beta>0 \qquad (3)$$

其中，$f_i(x)$为用户 i 的认证门限，ave 为用户成功认证时获得认证权重的均值，var 为用户成功认证时获得认证权重的均方差，β为调节系数，仅当用户身份认证成功或当认证失败后强制输入认证密码认证成功时，认证中心才更新用户的认证门限。重复此过程不断更新认证门限，使其适应用户习惯的变化。本文中取β=30。

5　实验分析

本文实验中数据使用 VAST 2008 公开数据集。VAST 2008 通话数据集是由 2008 VAST 竞赛提供的数据集，描述了 Catalano 社会网络的通话结构。其中包括 9 834 条记录、400 个节点和 961 条边[11]。实验中设定用户的好友上限数为 20，通话时间大于 10min 作为有效通话事件。VSAP 中各参数如上所述(θ=10(min), η=2, ξ=0.1, β=30)，SAP（即不考虑好友影响因子、认证票据权重、个人行为差异的认证方式）认证门限为认证票数大于等于 3。将 VAST 数据集作为系统输入，比较 VSAP 和 SAP 的认证性能，其中，SAP 结果如图 7 所示。

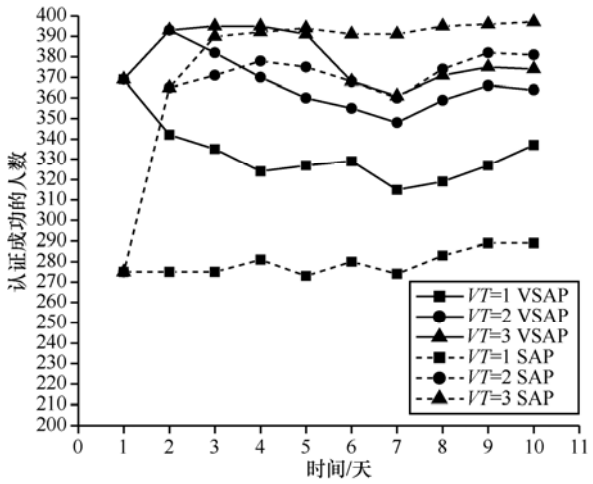

图 7　VSAP 与 SAP 认证成功人数对比（VT:认证票据有效期）

由图 7 得，2 种认证协议在认证票据有效期较长时，认证成功率都较高。但是随着认证票据的有效期增加，VSAP 认证成功人数的增加速度低于 SAP 的增加速度。VSAP 由有效期 1 天时认证成功人数远高于 SAP，至有效期 2 天时认证成功人数略低于 SAP,再到有效期 3 天时差距进一步扩大。

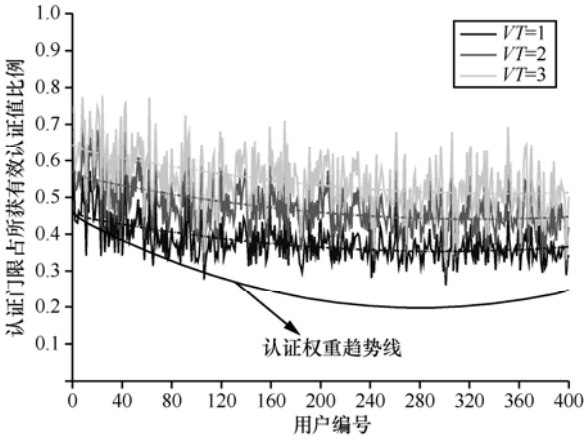

图 8　VSAP 认证门限占用户获得的认证权重比例
（VT：认证票据有效期）

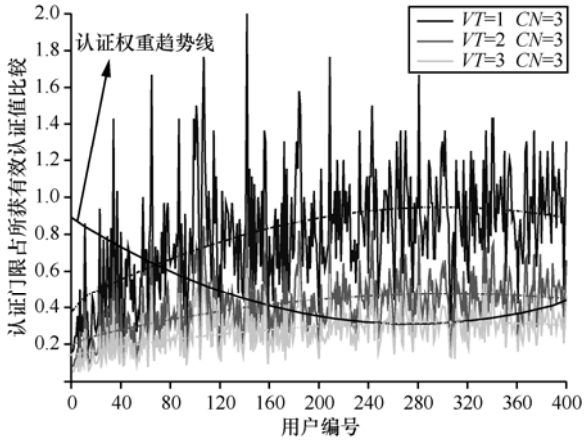

图 9　SAP 认证门限占用户获得的认证权重比例
（VT: 认证票据有效期，CN: 认证时要求的认证票据数）

通过对比图 8 和图 9 可知，随着认证票据的有效期增加，VSAP 中的 PATA 不断上升，而在 SAP 中的 PATA 却不断降低。由此可以得出在认证票据有效期较长时，SAP 是以牺牲认证的安全性来换取认证的成功率。当认证票据有效期较短时，SAP 由于认证门限是统一设定的，其中会出现认证门限比用户所能获得的认证权重高的现象，导致了 SAP 的认证成功率急剧下降，而 VSAP 却不同，由于其门限是根据用户所能获得的认证权重值计算获得的，正常情况下不会出现用户的认证门限比其能够获得的认证权重值高的现象，所以 VSAP 更加适合于

认证票据有效期短的环境中。由此便解释了图 7 中的现象。另一方面由图 8 和图 9 可知，VSAP 中用户获得的认证权重越高，则 PATA 也越高。SAP 中由于认证门限是统一设定的，还导致了当用户获得的认证权重越高时，其门限所占的比例就越低。用户获得的认证权重高反映了其频繁使用手机，由于频繁使用手机，则其对安全性要求相对较高。对于获得认证权重越高的用户，VSAP 认证时利用用户获得的认证票据数量就越多，而 SAP 却浪费的认证票据越多，显然 VSAP 认证的安全性更高，更能满足频繁使用手机的用户对安全性的需求。

从以上数据分析和实验结果中可知，本系统具有安全性高、对终端资源需求量小、适用性强的特点，尤其当要求认证票据有效期短和安全性要求高时，更能体现本系统高效的认证性能和优势。

6　结束语

本文提出了一种基于云计算的智能手机社交认证系统及认证协议。系统通过利用网络中存在的交互事件所携带的信任度不同、各好友的影响力不同、个体行为具有差异性的特点，将大量的存储和计算任务转移到云端，利用云计算的优势弥补了移动终端资源受限的缺陷，提高了用户的使用体验，改善社交认证的性能并增强了认证的安全性。实验表明本认证系统有效地提高了基于社交网络的认证方式在票据有效期短时的认证成功率，尤其适合与安全性要求高的场合，降低了对终端的资源消耗，并减少用户的操作提高了用户使用体验。但本文中由于数据集的限制，仅使用了通话记录作为认证条件。在下一步的工作中将考虑更多的认证条件，如短信、蓝牙等，进一步提高系统的认证成功率和安全性。

参考文献：

[1] FURNELL S, CLARKE N, KARATZOUNI S. Beyond the pin: enhancing user authentication for mobile devices[J]. Computer Fraud and Security, 2008, 2008(8):12-17.

[2] MAURO C, IRINA Z Z, BRUNO C. Mind how you answer me![A]. Proceedings of the 6th ACM Symposium on Information, Computer and Communications[C]. Hong Kong.China.2011.249-259.

[3] GUERRA-CASANOVA J, SÁNCHEZ-VILA C, BAILADOR G, *et al*. Authentication in mobile devices through hand gesture recognition[J]. International Journal of Information Security, 2012,11(2):65-83.

[4] TRESADERN P A, IONITA M C, COOTES T F, *et al*. Real-time facial feature tracking on a mobile device[J]. International Journal of Computer Vision, 2012, 96(3):280-289.

[5] CHOW R, JAKOBSSON M, MASUOKA R, *et al*. Authentication in the clouds: a framework and its application to mobile users[A]. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop[C]. Chicago, Illinoism, USA, 2010.1-6.

[6] BRAINARD J, JUELS A, RIVEST R, *et al*. Fourth factor authentication: somebody you know[A]. ACM CCS[C]. Alexandria Virginia, USA, 2006. 168-78.

[7] EGELMAN S S, REEDER R W, *et al*. It's not what you know, but who you know: asocial approach to last-resort authentication[A]. Proceedings of the 27th Annual SIGCHI Conference on Human Factors in Computing Systems[C]. Boston, Massachusetts, USA, 2009.1983- 1992.

[8] SOLEYMANI B, MAHESWARAN M. Social authentication protocol for mobile phones[A]. IEEE Computational Science and Engineering CSE'09 International Conference[C]. Vancouver, Canada, 2009. 436-441.

[9] Wikipedia[EB/OL]. http://en.wikipedia.org/wiki/Authentication, 2012.

[10] JOSANG A, ISMAIL R, BOYD C, *et al*. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems, 2007, 43(2): 618-644.

[11] YE Q, ZHU T, HU D, *et al*. Cell phone mini challenge award: social network accuracy exploring temporal communication in mobile call graphs[A]. IEEE Symposium on Visual Analytics Science and Technology[C]. Columbus, Ohio, USA, 2008.207-208.

作者简介：

刘宴兵（1971-），男，四川遂宁人，博士，重庆邮电大学教授、博士生导师，主要研究方向为无线网络管控和网络信息安全。

刘飞飞（1987-），男，江苏淮阴人，重庆邮电大学硕士生，主要研究方向为移动终端安全。