基于手机传感器的智能防盗与用户认证

赵银龙，宋　晖，任建军，吴西送

（东华大学 计算机科学与技术学院，上海 201620）

摘　要：本文提出一种新的智能手机防盗方案：根据用户掏手机动作过程中手机传感器产生的数据，使用DTW（动态时间规整算法）作为分类算法，然后用Boosting算法进一步提升分类的准确性。该方案不仅可以实时智能防盗，而且还可以进行用户认证。实验结果表明，该方案能达到令人满意的准确率。

关键词：智能防盗；用户认证；DTW算法；Boosting算法；行为特征

中图分类号：TP311　　**文献标识码**：A　　**文章编号**：2095-2163(2015)01-0101-05

Intelligent Antitheft and User Authentication based on Sensors of Smartphone

ZHAO Yinlong, SONG Hui, REN Jianjun, WU Xisong

(College of Computer Science and Technology, Donghua University, Shanghai 201620, China)

Abstract: This paper proposes a new scheme: according to the data produced by the phone's sensors during user's movement of picking phone out of pocket, use DTW as the classification algorithm, and then use the boosting algorithm to enhance the accuracy of classification. This scheme can not only provide intelligent antitheft timely but also provide user authentication. Experiments demonstrate that the scheme can achieve satisfactory accuracy.

Key words: Intelligent Antitheft; User Authentication; DTW; Boosting; Behavioral Traits

0　引　言

如今的智能手机更多地被用来管理个人信息（图片、日程安排、银行卡密码等）、使用手机银行等[1]。这些个人隐私信息的丢失和泄露会给用户带来较大隐患。如何保护手机上隐私信息的安全已经成为人们普遍关注和重视的热点问题。为此提出了各种各样的解决方案，主要分为两类：用户认证和手机防盗。用户认证即用户进入系统前通过某种方法来验证用户的合法身份，防止非法用户进入系统导致隐私信息泄露[2]。最常用的用户认证是使用密码、PIN或图案密码来进行身份识别。这种方法的缺点之一是密码越长越复杂、即越安全，但复杂的密码却难以记忆，而且对于短时间内多次进入系统导致的频繁解锁将造成用户使用上的十分不便。目前针对手机防盗采取的方案，大都属于事后采取措施降低损失的方法。通常是在发现手机丢失后发送指令远程锁定手机、备份数据、删除数据、远程定位、近距离控响警报等操作，但却仅仅能够降低数据丢失和泄露的风险，找回手机的可能性多会很小。

本文提出一种新的手机智能防盗方案，针对用户掏取手机这一过程，采集智能手机配备的加速度和角速度传感器数据，从这些数据中提取用户的行为特征值，根据特征值甄别这一动作。该方案根据掏取手机动作的传感器数据，能同时完成用户认证和手机的实时智能防盗功能，如果认证成功则自动解锁系统，认证失败则及时操控防盗警报、避免手机丢失。

1　相关工作

基于人体生物特征的认证方案如指纹识别、人脸识别、虹膜识别、视网膜识别等，相对于传统的密码方案具有更好的安全性和方便性。但是这类方案的缺点是需要特定的硬件支持（指纹识别器等），而且其中的人脸识别、虹膜识别则对周围的环境带有一定要求，再者如人脸识别可以通过使用面部静态照片实施伪造，指纹也可以实现复制。在进入智能手机时代后，手机除了有触摸屏之外还配备多种实用传感器，能够在使用手机期间获得更多的有用数据，而后通过数据挖掘算法，抽取一定的特征值进行用户行为特征识别认证。常见的基于行为特征的用户认证主要有：动态手势认证、语音识别、击键行为认证、步态认证、手机使用习惯认证等[3]。然而基于击键的用户认证，需要用户持续击键一段时间才能识别用户是否合法，而且这种击键的特征可能因为手机尺寸和输入法键盘布局的不同而有所变化，因而该种方法更加适合功能手机。并且这类认证方案仅能进行用户认证而不能用于手机防盗。

目前的手机防盗方案，主要是在用户发现手机丢失之后，通过某种形式远程发送指令备份数据、删除隐私数据、锁定手机、手机定位以及手机警报功能。这种方案的缺点是用户需要及时发现手机丢失，否则会导致信息丢失和泄露，而且通过定位和警报功能找回手机也颇为困难。

针对以上问题，本文提出基于掏兜动作手机传感器数据设计的方案，不仅能实现手机智能实时防盗，避免手机丢失，

收稿日期：2015-01-15

作者简介：赵银龙（1990-），男，河南周口人，硕士研究生，主要研究方向：手机安全、相似度查询；
宋　晖（1975-），女，上海人，博士，教授，主要研究方向：手机安全、Web信息挖掘、智能信息处理；
任建军（1989-），男，河南新乡人，硕士研究生，主要研究方向：手机安全、Web语义；
吴西送（1988-），男，安徽界首人，硕士研究生，主要研究方向：手机安全、相似度查询。

还能实现用户认证功能。

2 动态时间规整算法(DTW)

DTW[4]是把时间规整和距离测度结合起来的一种非线性规整技术。算法的输出是两个时间序列的最小距离,输出的值越小说明两个时间序列越相似。本文使用DTW算法对样本数据分类训练和认证识别。在样本训练阶段,假设训练样本集由 N 个样本组成,分别记为 T_1、T_2、T_3、$\cdots T_N$,使用DTW算法分别计算训练样本集中任意两个样本之间的距离,选取其中的最大值 max*Dist* 作为训练样本集的模板特征。max*Dist* 的计算公式如下:

$$\max Dist = \max_{i,j=0}^{N} \{ DTW(T_i, T_j) \} \quad (1)$$

在测试样本识别阶段,用DTW分别计算测试样本和训练模板中每一个样本的相似度距离并记为 $D_i, i = 1 \cdots N$。若这些 D_i 值中有半数以上小于此训练模板的 max*Dist* 值,则该测试样本识别成功。即满足以下公式的测试样本识别成功:

$$|\{D_i | D_i < \max Dist, i = 1 \cdots N\}| > \frac{N}{2} \quad (2)$$

3 Boosting 算法

Boosting[5]算法可以将若干个弱分类器组合起来,变成一个强分类器。弱分类器指识别错误率小于1/2的学习算法。识别准确率很高并能在多项式时间内完成的学习算法称为强学习算法。Boosting算法使用弱分类算法产生基分类器,对分类错误的样本分配更大的权值,并在下次分类时重点对分类错误的样本进行处理。最后对这些弱分类器进行加权整合得到最终的强分类器。各个弱分类器的识别率不同,识别率越高的弱分类器权重越高,识别率越低的基分类器权重越低。

4 实验与结果分析

由于寻找弱分类器要比强分类器容易很多,通过Boosting算法可以提高弱分类器的准确率。因此,本文首先使用DTW作为弱分类算法,对数据进行初步分类。然后用Boosting算法对用DTW得到的弱分类器加权整合为强分类器,并与未整合之前的弱分类器作对比。整体实验过程如图1所示。

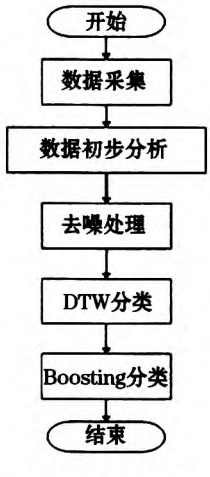

图1 实验流程

Fig. 1 Experimental process

4.1 数据采集程序

研究开发了一款基于Android平台的数据采集APP程序。程序采集掏兜动作过程手机加速度传感器、角速度传感器数据。程序有三个控制按钮,开始按钮即启动本次数据采集,结束按钮则终止本次采集,当再次按下开始按钮将重新启动下一次的数据采集,直到本次所需的样本数目足够时,对应按下退出键结束程序执行。为方便程序的使用,程序的开始和暂停也可以通过音量键的上下键来控制。数据采集程序运行图则如图2所示。

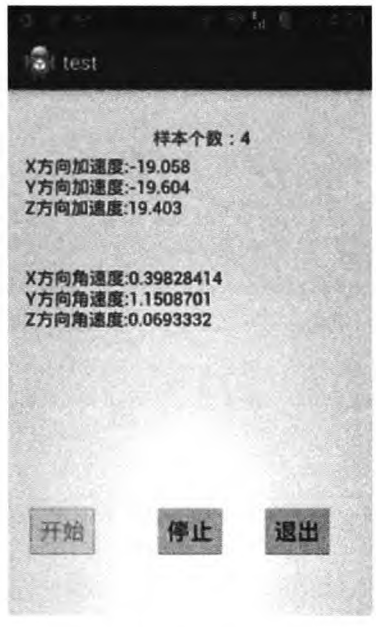

图2 程序界面

Fig. 2 Program UI

4.2 数据采集

参与数据采集的用户共有20人,其中15名男生,5名女生,每个人采集50个样本数据。使用每人50个样本中的40次作为训练样本,根据构建的分类模型训练分类器,另外10次组成大小为200的识别样本集以验证分类器的准确度。

4.3 数据初步分析

为验证方案的可行性,首先对样本数据进行初步处理。绘制原始数据的时间序列图,对每个人的样本数据集按照加速度、角速度传感器的 X、Y 和 Z 三个方向的数据分别绘制时间序列图。图3(a)和图3(b)分别为两个不同用户 X 方向加速度10次样本数据的时间序列图。从图中可以看出同一用户不同样本数据 X 方向加速度时间序列图具有明显的相似性,不同用户样本时间序列图有明显的差异性。通过观察其他用户其它传感器数据的时间序列图可以得到相同的结论。

4.4 噪声去除

从图3(a)和图3(b)中可以看到时间序列图不太平滑,有一些点明显有些偏离,这是由噪声导致的。本文使用低通滤波器处理样本数据,过滤掉高频噪声。对样本数据进行FFT快速傅里叶变换将样本数据从时域转换到频域。图4所示为未使用SMA过滤的 X 方向加速度时间序列图。图5

所示为 X 方向加速度一个样本数据转换的频域图。从图中可以看出,大部分数据频率低于 10HZ,高于 10HZ 的数据是高频噪声。使用 SMA(simple moving average)过滤器对样本数据进行处理。图 6 所示即为使用 SMA 过滤后的 X 轴加速度时间序列图,图 7 所示则为对 SMA 过滤后的样本数据进行 FFT 变换得到的频域图。对比图 4 和图 6 可知 SMA 过滤之后的时间序列图相比未过滤率之前更加平滑。对比图 5 和图 7 将会发现高于 10HZ 的噪声数据基本被过滤掉。

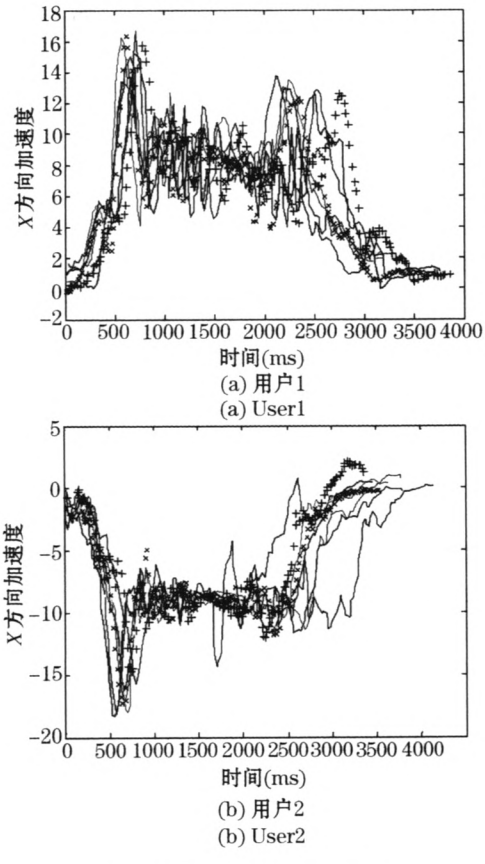

图 3 不同用户的时间序列图

Fig. 3 Time sequence diagram of different users

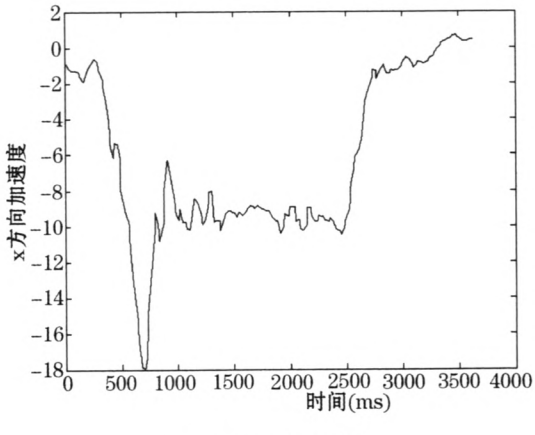

图 4 未去噪时序图

Fig. 4 Not denoising time sequence diagram

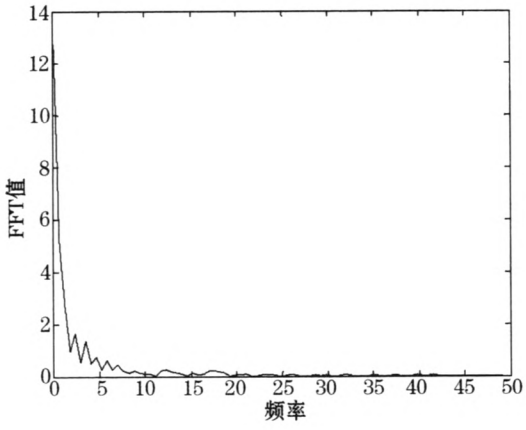

图 5 未去噪频域图

Fig. 5 Not denoising frequency – domain diagram

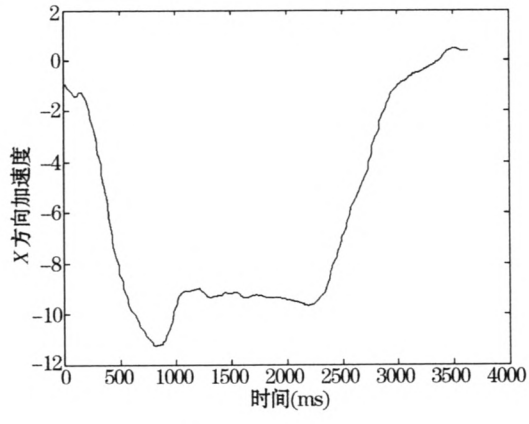

图 6 去噪时序图

Fig. 6 Denoising time sequence diagram

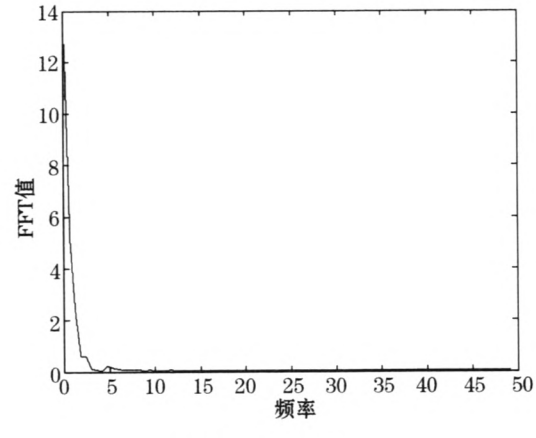

图 7 去噪频域图

Fig. 7 Denoising frequency – domain diagram

4.5 DTW 算法初步分类

图 8 和图 9 分别为 X 方向加速度的两个样本数据在 DTW 规整前和规整后的时间序列图,规整后两个样本数据时序图几乎完全一致,可见 DTW 能够尽可能减小时间位移对相似性计算的影响。

使用该方法对样本数据加速度和角速度的 X、Y、Z 三个方向上的值分别进行分类模板训练和测试样本识别,得出加速度与角速度在 X、Y、Z 方向上的 6 个分类器的分类结果。

本文使用认证系统性能评价中常用的两个指标：*FAR*(False Alarm Rate)和 *IPR*(Impostor Pass Rate)评价分类器的性能。图10所示为这6个分类器的 *IPR* 和 *FAR* 值。

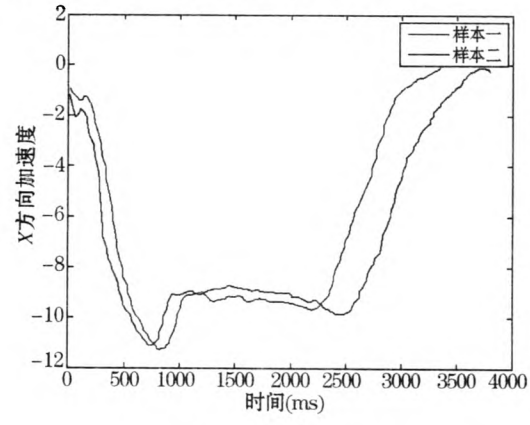

图8 规整前时序图

Fig. 8 Time sequence diagram before regular

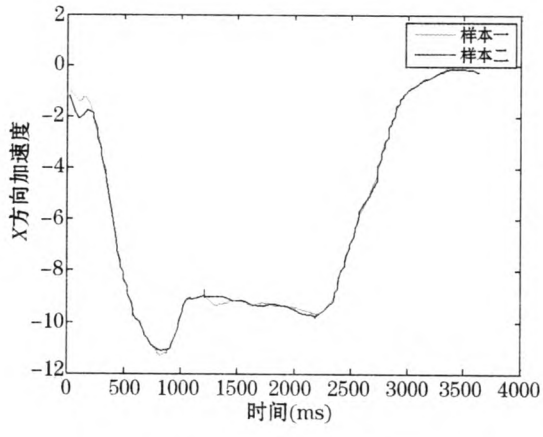

图9 规整后时序图

Fig. 9 Time sequence diagram after regular

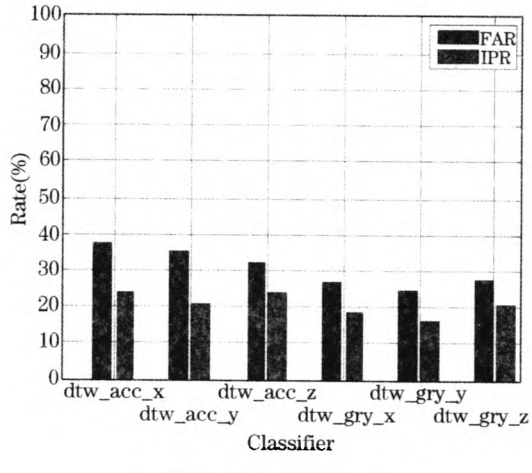

图10 分类器准确率

Fig. 10 Classification accuracy

观察该图可见六个分类器中 dtw_gry_y(*Y* 方向角速度)的 *FAR* 最低为25%，*IPR* 也最低为16.5。六个分类器得到的 *FAR* 介于25%～38%，*IPR* 值介于16.5～24%。相比于其它认证方法，如步态认证得到 *EER*(Equal Error Rate)为7%，击键认证的 *EER* 为12.8%，仅仅使用DTW方法对样本数据进行识别的结果还不够理想。

4.6 使用 Boosting 算法及类比同类认证

使用DTW的分类器正确率为62%～75%，属于较弱分类算法。本文使用 Boosting 算法来提升这些弱分类器的准确率。图11所示为使用 Boosting 算法得到的 *FAR*、*IPR* 和直接由DTW分类的六个弱分类器的 *FAR*、*IPR* 对比柱状图。

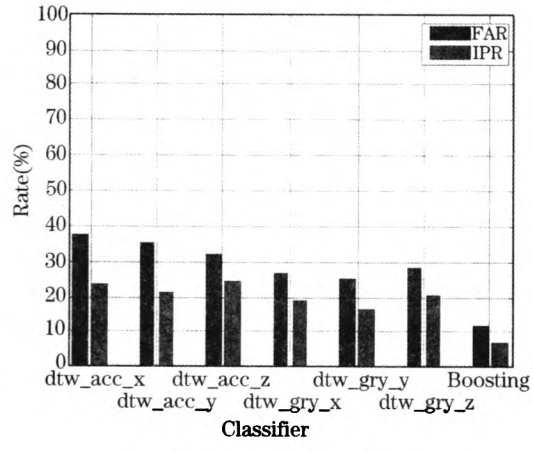

图11 Boosting 与弱分类器

Fig. 11 Boosting and weak classification

由图可见，使用 Boosting 对 DTW 分类器加强后的 *FAR* 为12%，*IPR* 为7.5%，和步态识别认证(*EER* 为7%)以及击键认证(*EER* 为12.8%)的准确率相近。但是步态识别认证需要相对较长的时间才能完成一次认证，而本文的方法在训练后只需要一次掏兜动作即可完成认证。同样地，对于击键认证方法也需要一段时间的击键动作才能收集到判断是否为合法用户的足够数据，而且应用于智能手机上的击键认证的准确率不如在电脑上高，且将受具体的虚拟键盘的布局的影响。

5 结束语

本文提出的基于智能手机掏兜动作识别方案，能够同时实现手机智能实时防盗和透明用户认证。样本数据分类训练完毕后，用户某次的掏兜动作数据作为测试样本进行识别，识别成功则手机自动解锁，省去用户手动解锁操作；识别失败则及时警报铃声，避免手机丢失带来财物和信息损失。目前研究的不足之处是，Boosting 之后的准确率还可以进一步提高，有待于在下一阶段工作中改进。

参考文献：

[1] SHAHZAD M, LIU A X, SAMUEL A. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it [C] // Proceedings of the 19th ACM Annual International Conference on Mobile Computing and Networking 2013, Florida: MobiCom, 2013:39-50.

[2] O'GORMAN L. Comparing passwords, tokens, and biometrics for user authentication [J]. Proceedings of the IEEE, 2003, 91(12): 2021-2040.

(下转第108页)

理控制台来操作和完成。该控制台的功能实现可表述为:信任策略用于在两个以上域或不同群集中建立信任关系;权限策略模板可以根据用户的不同需求预先制定不同安全权限的策略模板,需要时可直接调用;而权限账户证书策略则用来配置 AD RMS 服务器颁发给每个客户的认证凭证(包含一个公钥)的有效期;另外,AD RMS 排除策略主要是用来防止非授权用户使用 AD RMS 服务,包括用户排除、应用程序排除、密码箱排除等;此外,还有安全策略包括超级用户、群集密钥密码和解除授权,但在默认状态下,所有策略却都是禁用的,因而配置之前必须将其启用。

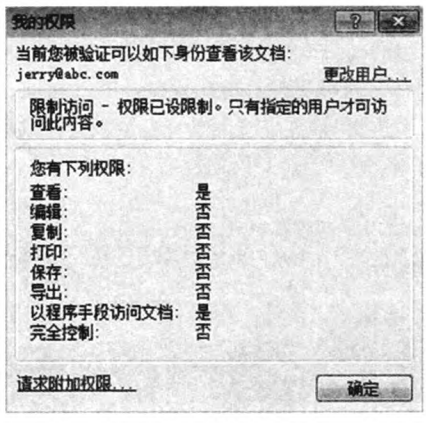

图 10 权限列表

Fig. 10 Permissions list

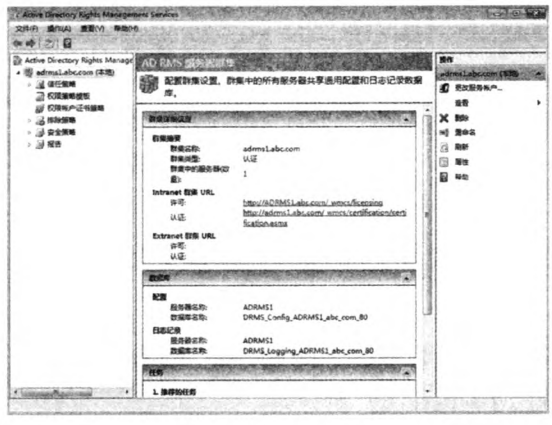

图 11 AD RMS 管理控制台

Fig. 11 Admin console of AD RMS

3 结束语

AD RMS 服务的应用简明清晰,本文搭建的是测试环境。在真正的生产环境中部署 AD RMS 系统时,要将 AD RMS 服务单独安装至一台服务器,如果条件不能满足,AD RMS 服务与域控制器将在同一服务器上,此时就必须将 AD RMS 服务账号添加到域管理员用户组中。数据库服务也要使用微软的 SQL Server ,Windows 服务器上的内部数据库服务却仅适用于测试环境。AD RMS 客户端通过网络与群集通信时,使用 SSL 加密的连接将更为安全,并且确保安装了证书服务器。AD RMS 服务器安装完毕,则要及时备份并将群集密钥密码置于妥善、安全的管理之下。

参考文献:

[1]杨敏. 企业信息安全管理体系建设的探讨[J]. 电子技术与软件工程,2013(24):238 - 239.

[2]赵林. 计算机网络信息安全及防护策略研究[J]. 网络安全技术与应用,2014 (3):159 - 160.

[3]Microsoft. Active Directory 权限管理服务[EB/OL]. http://technet. microsoft. com/zh - cn/library/cc771627. aspx,2008(7).

[4]戴有炜. Windows Server2008R2 安装与管理[M]. 北京:清华大学出版社,2011(1):404 - 420.

[5]王星亮. 计算机网络安全中数据加密技术的应用分析[J]. 计算机光盘软件与应用,2013(13):169 - 170.

(上接第 104 页)

[3]JAKOBSSON M, SHI E, GOLLE P, et al. Implicit authentication for mobile devices [C] // Proceedings of USENIX Summit on Hot Topics in Security 2009, Montreal: HotSec, 2009:9 - 14.

[4]BERNDT D J, CLIFFORD J. Using dynamic time warping to find patterns in time series [C] // Proceedings of KDD Workshop, Seattle, WA:AAAI Press, 1994:359 - 370.

[5]BUHLMANN P, HOTHORN T. Boosting algorithms: regularization, prediction and model fitting [J]. Statistical Science, 2007,22(4): 477 - 505.