# 面向智能手机的自适应触屏持续认证方案

姜 奇[1,2],文 悦[1],张瑞杰[3],魏福山[2,4],马建峰[1]
(1. 西安电子科技大学网络与信息安全学院,陕西西安710126; 2. 河南省网络密码技术实验室,河南郑州450001; 3. 战略支援部队信息工程大学密码工程学院,河南郑州450001; 4. 战略支援部队信息工程大学网络空间安全学院,河南郑州450001)

**摘 要:** 近年来,智能手机的触屏认证受到了广泛的关注. 现有的认证方案在受外界环境影响时认证能力会下降,为提高认证的稳定性和安全性,本文对基于触屏时触控传感器行为和运动传感器行为的双模态认证进行了研究. 然而,双模态认证系统复杂度增加且会带来大量的资源消耗,因此,本文提出一种自适应触屏持续认证方案. 其可根据上下文参数自适应地选择不同强度的认证策略,达到了降低认证系统复杂度以及能耗的目的,实验表明该方案在提供足够设备安全性的同时使能耗降低50%以上.

**关键词:** 持续认证; 自适应; 触屏行为; 分数级融合; 运动传感器; 触控传感器
**中图分类号:** TP391.4 **文献标识码:** A **文章编号:** 0372-2112(2022)05-1131-09
**电子学报URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210624

# An Adaptive Touchscreen Based Continuous Authentication Scheme for Smart Phones

JIANG Qi[1,2], WEN Yue[1], ZHANG Rui-jie[3], WEI Fu-shan[2,4], MA Jian-feng[1]
(1. *School of Cyber Engineering, Xidian University, Xi'an, Shaanxi* 710126, *China*;
2. *Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan* 450001, *China*;
3. *School of Cyber Engineering, Information Technology University, Zhengzhou, Henan* 450001, *China*;
4. *School of Cyber Science and Engineering, Information Technology University, Zhengzhou, Henan* 450001, *China*)

**Abstract:** Touchscreen-based authentication has received widespread attention for smart phone. Since the existing authentication schemes are vulnerable to the external environment, we mainly study the dual-modal authentication including touch sensor behavior and motion sensor behavior when touching the screen, so as to improve the security of authentication. However, the complexity of the dual-modal authentication system increases; and will bring a lot of CPU(Central Processing Unit) resources and power consumption. Therefore, we propose an adaptive touch screen continuous authentication method, which can adaptively select the authentication strength according to the context, and reduce the complexity and energy consumption of the authentication system by avoiding the use of motion sensor behavior authentication when the touch screen is used. And experiments show that the method can reduce energy consumption by more than 50% while providing sufficient smartphone safety.

**Key words:** continuous authentication; adaptive; touchscreen; score-level fusion; motion-sensor; touch-sensor

## 1 引言

智能手机的持续认证方法日益受到关注[1~3]. 由于触屏操作的通用性和普遍性,以及用户间在触摸屏交互过程中的行为模式具有较高的独特性,因此是作为持续认证因子的最佳选择之一.

目前,针对触屏操作行为认证的研究主要基于两类传感器行为:一种是触屏时触控传感器行为[4,5],其主要利用设备的触摸屏获取触屏时手指压力、指尖覆盖面积和位置等信息. Frank等[4]使用触控数据进行持续身份认证,达到了等错误率(Equal Error Rate, EER)低于4%的效果. Fierrez等[5]分别使用支持向量机(Support Vector Machine, SVM)算法、高斯混合模型以及SVM和高斯混合模型进行了基准测试,结果表明横屏触屏操作认证性能好于竖屏触屏操作以及水平滑动认

收稿日期:2021-05-17;修回日期:2021-08-17;责任编辑:覃怀银
基金项目:国家自然科学基金(No.62072352, No.61772548, No.61872449);陕西省教育厅科研计划项目资助(No.20JY016);中央高校基本科研业务费资助项目

证优于垂直滑动；另一种是触屏时运动传感器行为[6~9]，其主要利用设备内置的运动传感器捕获触屏操作引起的设备抖动和方向变化. Lee 等[9]提出了基于多运动传感器的方案实现对智能手机的持续身份认证，其使用SVM实现了高达90%的准确率. Shen 等[6]提取触屏操作发生时加速度计、磁力计、陀螺仪和方向感应计等运动传感器数据的时域和频域特征，实现了5.03%的错误拒绝率(False Reject Rate, FRR)和3.98%的错误接受率(False Accept Rate, FAR).

但是，研究表明，单模态行为认证本身易受环境和情绪等不可控因素的影响，导致认证能力不稳定[10]. 此外，触屏时触控传感器行为和运动传感器行为被证明会遭受模仿[11]和统计攻击[12]. 而融合上述两种行为的双模态行为认证预期可以克服单模态行为认证的上述缺点[6,13]. 具体而言，同时利用两种行为对用户进行认证，可以在一种行为认证能力下降时使用另一种行为进行弥补；而且双模态认证系统可以增加模仿攻击和统计攻击的难度. 因此，双模态融合能够在增强认证系统稳定性的同时增加安全性.

然而，相对于单模态利用单一行为进行认证，双模态认证需要同时利用两种行为进行认证，增加了系统的复杂性. 此外，同时对多个来源的数据进行监控采集和处理，尤其是触屏时运动传感器行为需要监控多个传感器，包括加速度计、陀螺仪和磁力计，会带来大量的中央处理器(Central Processing Unit, CPU)资源和电量消耗，势必影响到用户使用体验. 考虑到智能手机的私有性，即在大多数情况下设备的使用用户是设备的拥有者. 而每个用户有自己的生活习惯和应用程序使用习惯；此外用户在使用不敏感的应用程序时，比如天气、计算器等，无需启用高安全强度的持续认证方式. 因此，本文提出了根据上下文自适应选择适当的持续认证机制，其可以提高认证系统的可用性，更有利于促进持续认证系统的推广应用. 实验表明，该方案可以提供足够的安全性，且可以通过减少使用双模态认证来降低认证系统复杂性的同时使能耗降低50%以上.

## 2 自适应触屏持续认证方案

如图1所示，本文提出一个自适应触屏持续认证方案. 当用户启动某个应用程序时，该方案会利用自适应模型根据当前上下文参数进行环境安全水平评估，进而选择触屏认证策略. 方案支持两种认证策略，分别是单模态触屏行为认证和双模态触屏行为认证. 单模态认证可以利用触屏触控传感器行为或触屏运动传感器行为进行认证，双模态认证则融合上述两种行为进行认证，本文采用分数级融合. 双模态认证的优势在于可提高认证准确性，但是其缺点在于系统复杂度及能量消耗高. 为此，自适应模型的作用是根据当前用户的上下文参数自适应地选择触屏认证策略，即在上下文安全水平较高时选择单模态认证，而在上下文安全性水平较低时使用融合触控传感器行为和运动传感器行为的双模态认证，达到在保证安全性的同时降低认证系统复杂度和能量消耗的目的.

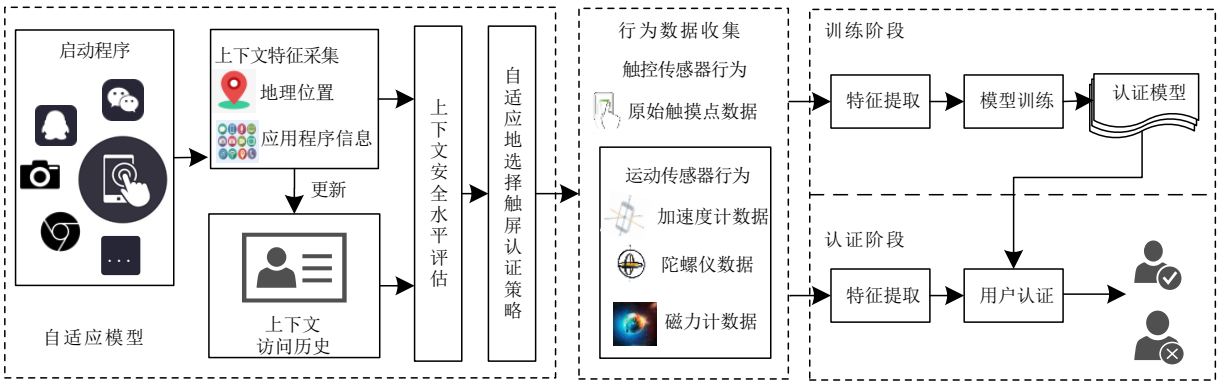



图1 自适应触屏持续认证系统流程图

### 2.1 触屏持续认证

当用户与智能手机正常交互时，触屏操作就会发生，且用户之间的触屏方式具有独特性. 同时，当用户进行触屏操作时会引起手机抖动，手机内置的运动传感器可以捕捉这类行为并提供手机旋转和位移等信息. 本节探讨了以上两种行为分别在单模态以及在融合两种行为的双模态下的认证能力.

#### 2.1.1 数据收集和特征提取

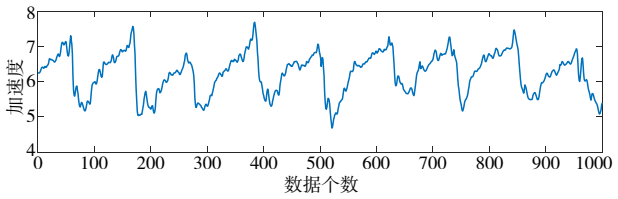
(1) 触屏时触控传感器行为

通过智能手机操作系统的应用程序编程接口(Application Programming Interface, API)可获得触控点坐标、手指覆盖面积及压力等原始触摸点数据，然后可提取出区分用户行为模式的特征，从而准确的识别用户. 对于每次的触控传感器行为，我们从中提取了25个不

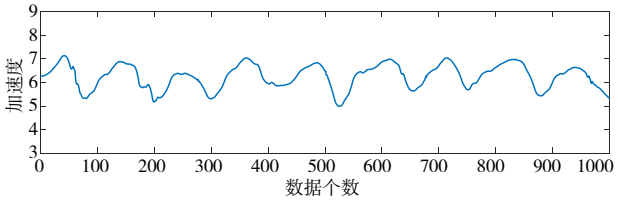
同的特征,包括:触屏滑动的开始和结束触摸点坐标、触屏滑动端到端的直线距离和和滑动轨迹的长度及它们之间的比值、端到端成对相邻触摸点速度和加速度的平均值和标准偏差及其20%,50%,80%的百分位数、端到端成对相邻触摸点标准偏差的最大值,标准偏差,及其20%,50%,80%的百分位数、触屏滑动时间和指尖压力大小和面积等.

(2) 触屏时运动传感器行为

通过加速度计,磁力计和陀螺仪等3种运动传感器获取的三维数据序列刻画触屏操作引起的行为变化.对原始传感器数据的处理如下:首先,对原始数据序列进行数据内插和去噪等预处理操作,处理前后的数据变化如图2所示.其次,从三个传感器的$X,Y,Z$以及幅度$M$轴提取时域特征,其中$M=\sqrt{x^2+y^2+z^2}$,与手机设备以及触屏的方向无关,表示触屏时振动的幅度.最后,为了降低提取的特征维度,依据每个特征的fisher score进行特征选择.表1列出了提取的时域特征以及三个传感器四个纬度的fisher score情况.我们选择了所有fisher score大于0.1的特征进行后续的操作.




(a) 预处理前




(b) 预处理后

图2　手机加速度计$x$轴预处理前后数据变化

### 2.1.2　模型训练和用户认证

该系统支持两种认证策略,分别是单模态触屏行为认证和双模态触屏行为认证.单模态认证分别利用触屏触控传感器行为、触屏运动传感器行为进行认证,双模态认证融合上述两种行为进行认证.

在模型训练阶段,我们利用五种常见的监督式学习算法分别根据上述两种行为提取的特征进行认证模型的训练,包括SVM、K近邻算法(K Nearest Neighbor, KNN)、多层感知机(Multi-Layer Perceptron, MLP)、随机森林(Random Forest, RF)以及极端梯度提升算法(Extreme Gradient Boosting, XGBoost).

在认证阶段,系统根据所选择的认证策略,在用户使用设备期间持续收集对应的行为数据,在提取特征后,使用训练的认证模型对用户进行认证.如认证成功,则用户正常使用智能手机;反之,认证失败则需要进行显示的用户认证,如用户手动输入口令或者短信验证码等方式.

在使用上述单模态认证的基础上,我们选择相应性能最好的分类器对两种行为进行融合认证.由于分数级融合相对于其他融合方式具有易获取、包含的认证信息多、以及融合过程简单且可扩展,便于增加和减少模态等优点[14].本文采用了基于权重的分数级融合,具体方法如下所示:

$$s=w_1s_1+w_2s_2 \tag{1}$$

其中,$s$指最后的决策分数,$s_i$表示两种行为模态,$w_i$表示两种行为模态的分数权重$i=\{1,2\}$.在融合时,单模态认证能力强的行为将会获得较高的权重,反之将获得低的权重,计算方式如下:

$$d_i=\frac{\mu_i^G+\mu_i^I}{\sqrt{(\delta_i^G)^2+(\delta_i^I)^2}} \tag{2}$$

其中,$G$和$I$分别表示合法用户和非法用户,$\mu_i$与$\delta_i$分别表示分数的均值和方差,$d_i$表示单个行为的合法用户和非法用户的得分的分离程度.权重$w_i$与$d_i$成正比,分离程度越大,说明该行为认证能力更好,因此权重更大.

**表1　针对每一次触屏操作,运动传感器行为提取的特征以及相应的fisher score值**

| 特征 | 描述 | fisher score($A_X,A_Y,A_Z,A_M,M_X,M_Y,M_Z,M_M,G_X,G_Y,G_Z,G_M$) |
|---|---|---|
| 最大值 | 触屏滑动期间传感器读数最大值 | (0.35,0.86,0.49,0.33,0.35,0.460.41,0.37,0.17,0.11,0.08,0.12) |
| 最小值 | 触屏滑动期间传感器读数最小值 | (0.38,0.76,0.59,0.36,0.35,0.47,0.41,0.38,0.15,0.11,0.06,0.05) |
| 平均值 | 触屏滑动期间传感器读数平均值 | (0.43,0.90,0.69,1.00,0.35,0.47,0.41,0.37,0.03,0.02,0.01,0.07) |
| 标准差 | 触屏滑动期间传感器读数标准差 | (0.11,0.13,0.18,0.17,0.08,0.11,0.11,0.09,0.15,0.12,0.09,0.11) |
| 能量 | 触屏滑动期间传感器读数强度 | (0.64,0.72,0.78,0.97,0.23,0.19,0.32,0.31,0.05,0.05,0.03,0.05) |
| 偏差 | 触屏滑动操作前后传感器读数差异 | (0.01,0.02,0.02,0.01,0.01,0.01,0.05,0.01,0.41,0.02,0.07,0.01) |
| 净变化 | 触屏滑动操作引起的传感器读数变化 | (0.01,0.01,0.18,0.01,0.06,0.10,0.08,0.01,0.01,0.07,0.01,0.05) |
| 最大改变 | 触屏滑动操作引起的传感器读数的最大变化 | (0.07,0.11,0.13,0.14,0.04,0.05,0.09,0.04,0.11,0.09,0.07,0.10) |

### 2.2 自适应模型

双模态融合会增加认证的复杂性同时也会给智能手机造成能量消耗,因而需要提出自适应模型以降低资源开销,提升用户体验. 研究表明,用户的地理位置和应用程序使用习惯遵循一种可以预测的模式[15~17]. 每个用户偏好的应用程序不同,且对于相同的应用程序,用户间的使用频次和时长也具有不同的规律;除此之外,用户使用的应用程序愈来愈多,但不是所有的应用程序都存储用户的隐私数据. 因此,在用户熟悉的环境或使用不敏感应用时,可以降低持续认证的要求,仅仅使用耗能低的触屏时触控传感器行为认证;相反,如果在从未访问过的位置使用敏感程度高的应用或者从来没有使用过的应用,才需要更安全的双模态融合的方式.

因此,提出一种应用程序级自适应模型. 当用户启动应用程序时,根据上下文(地理位置和应用程序信息)自适应选择触屏认证因子,即确定当前所需要的认证模式,通过避免使用触屏时运动传感器行为认证达到降低系统复杂性和能量消耗的目的. 自适应模型包括3部分,分别是:上下文安全水平评估、上下文参数处理和计算、以及考虑应用程序对用户重要程度进行认证策略选择.

#### 2.2.1 上下文安全水平评估模型

上下文安全水平是自适应的依据,其由当前用户在当前上下文是合法用户的可信度来进行表征. 模型所涉及到的符号定义如下:$\boldsymbol{x}=(x_1,x_2,\cdots,x_d)$,表示打开某个应用程序时一组$d$维的上下文特征向量(在本文中,$d=2$,包括当前地理位置和应用程序名称). $u\in\{L,I\}$表示当前使用设备的用户的身份,其中$L$和$I$分别表示使用用户为合法用户和非法用户. $X$和$U$分别为$\boldsymbol{x}$和$u$的随机变量.

给定一组上下文特征向量$\boldsymbol{x}$,对于合法用户和非法用户两个类别,当满足以下条件时,有$U=L$:

$$\frac{p(U=L|X=\boldsymbol{x})}{p(U=I|X=\boldsymbol{x})}>1 \tag{3}$$

反之,$U=I$. $p(U=L|X=\boldsymbol{x})$表示在给定一组上下文特征向量$\boldsymbol{x}$条件下,使用用户是合法用户的概率,$p(U=I|X=\boldsymbol{x})$表示给定一组上下文特征向量$\boldsymbol{x}$,使用用户是攻击者的概率. 根据贝叶斯理论,式(3)能够被转化为式(4)的形式:

$$\frac{p(U=L|X=\boldsymbol{x})}{p(U=I|X=\boldsymbol{x})}=\frac{p(X=\boldsymbol{x}|U=L)p(U=L)}{p(X=\boldsymbol{x}|U=I)p(U=I)}>1 \tag{4}$$

由于$p(U=L)$和$p(U=I)$独立于$\boldsymbol{x}$,式(4)可写为:

$$\frac{p(X=\boldsymbol{x}|U=L)}{p(X=\boldsymbol{x}|U=I)}>\frac{p(U=I)}{p(U=L)} \tag{5}$$

$p(X=\boldsymbol{x}|U=L)$和$p(X=\boldsymbol{x}|U=I)$分别代表着合法用户和非合法用户在一组上下文特征向量为$\boldsymbol{x}$时的概率. 合法用户在上下文特征中的概率分布情况可以通过智能手机的日常使用历史中获得,但是攻击者的概率分布情况很难调查,这里假设敌手在所有上下文的出现概率相同,即服从于均匀分布. 因此,式(5)可以写为:

$$\underbrace{p(X=\boldsymbol{x}|U=L)}_{g_u(\boldsymbol{x})}>\underbrace{\frac{p(U=I)}{p(U=L)}}_{\theta}p(X=\boldsymbol{x}|U=I) \tag{6}$$

式(6)表示当$g_u(\boldsymbol{x})>\theta$时,$U=L$;反之,则$U=I$,阈值$\theta$能够相应的进行调整. $g_u(\boldsymbol{x})$为给定的一组上下文特征向量下,当前用户是合法用户的可信度得分. 根据此定义可知,当用户在更熟悉的上下文中使用手机设备时,$g_u(\boldsymbol{x})$更大. 因此,可以使用$g_u(\boldsymbol{x})$来表征合法用户在当前上下文下的安全水平. $g_u(\boldsymbol{x})$越大,说明对于合法用户来说,该环境更安全,即安全水平更高;反之,则安全水平低.

实际应用中,$g_u(\boldsymbol{x})$的计算是具有挑战的,因为$\boldsymbol{x}=(x_1,\cdots,x_d)$的组合情况是非常多. 为了克服这种情况,可假设所有的上下文特征是独立的,即:

$$p(\boldsymbol{x})=\prod_{k=1}^{d}P(x_k) \tag{7}$$

因此,式(6)的左边的计算方式为:

$$g_u(\boldsymbol{x})=p(x_1,\cdots,x_d|U=L)=\prod_{k=1}^{d}p(x_k|U=L) \tag{8}$$

因此,我们只需计算用户在单个上下文特征下的概率分布情况即可.

#### 2.2.2 上下文参数处理和计算

为了计算式(8)只需计算合法用户在相应上下文特征下的概率分布. 本文使用的上下文特征为地理位置和应用程序名称,因此需要计算合法用户在具体地理位置使用智能手机的频次以及使用具体应用程序的频次.

对于使用历史中出现的上下文,只需根据使用频次计算相应概率即可. 用户每打开一次应用程序,相应使用频次加1. 对于地理位置,使用全球定位系统(Global Positioning System, GPS)获取到的是当前位置的经度和纬度,是一个连续的值,可能组合的情况很多,不能使用频次来表示. 为此,我们将纬度和经度空间划分为离散的0.002×0.002纬度/经度网格[18],每个网格约为200 m×200 m,同一网格范围内的所有坐标对均标记为相同位置,划分表示如图3所示.

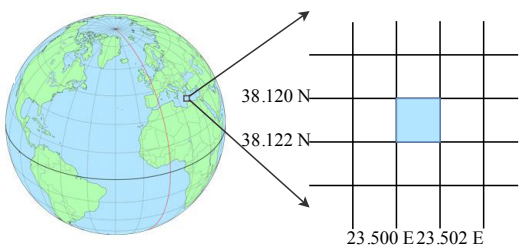



图3 GPS经纬度数据的处理

对于首次出现的上下文,即用户从来没有去过的地点或从未使用过的应用程序,对应的上下文安全水平永远等于0,这与实际情况不符. 例如,当用户在家想要尝试一个新的应用程序,这时的安全水平不仅与应用程序有关,还与地理位置有关. 本文利用数据平滑技术[19]解决该问题,其基本思想是减少已知特征值的概率,为未知特征值保留一些概率.

综上,最终的概率估计结果为

$$p(x_k|U=L)=\begin{cases}\dfrac{c(x_k)}{N}\left(1-\dfrac{1}{N+1}\right), & c(x_k)>0\\ \dfrac{1}{N+1}, & \text{其他}\end{cases} \tag{9}$$

其中,$c(x_k)$是在第$k$维上下文特征下,特征值$x_k$发生的次数,$N=\sum c(x_k)$是第$k$维上下文特征下,所有可能的特征值发生的总次数.

计算式(8)后,由于乘积之后的数值较小,不利于之后的计算,因而对$g_u(x)$进行了最大最小归一化处理,使安全水平映射在[0,1]之间.

#### 2.2.3　自适应认证策略选择

确定了上下文的安全水平后,不能直接选择不同的认证策略,此方式忽略了使用的应用程序的重要程度,即认证策略的强度不仅与当前环境的安全水平有关,还应该与用户对当前使用的应用程序保护程度相关. 用户认为很重要的应用程序应该采用更强的认证手段,反之,则相反. 为了将两种情况都进行考虑,本文设计的模型如下:

$$f(\boldsymbol{x},v)=\frac{1}{v}+g_u(\boldsymbol{x})+\frac{g_u(\boldsymbol{x})}{v} \tag{10}$$

其中,$v$指用户对使用的应用程序的保护程度,用户认为某个应用程序愈重要时$v$愈大.$f(\boldsymbol{x},v)$是综合考虑上述介绍的两种情况后的得分,基于此得分,系统自适应地选择不同强度的持续认证方式.$f(\boldsymbol{x},v)$的得分较高,说明用户当前所处的环境安全等级较高或者使用的应用程序不是很重要,此时可以使用简单且能耗低的单模态持续认证. 而当处于不熟悉的环境或者使用重要的应用程序(如手机银行)时会切换到更安全可靠的双模态认证.

部署了上述自适应模型之后,无论在何时何地均有不同强度的持续认证手段进行保护. 熟悉模仿攻击或统计攻击的专业敌手,对于单模态的攻击只会得到用户认为不重要的信息,而对于多模态的攻击难度增加. 综上所述,该系统能够在节省能耗的同时保证各种情况下系统的安全性.

## 3　实验结果与分析

### 3.1　触屏持续认证评估

本节评估了触屏时触控传感器行为和运动传感器行为的认证能力,每一种行为分别使用了第3节介绍的5种分类器进行认证测试,采用网格搜索法确定了所有分类器最好性能的超参数,然后对数据集中每一位用户进行训练和测试,汇总结果决定总体的认证能力. 同时,为了对比两种行为在不同运动状态下的鲁棒性,我们评估了用户坐着和步行两种运动状态下的性能变化. 最后,我们使用两种行为单模态下获得最好性能结果的分类器进行了两种行为模式的融合实验,对比分析了双模态和单模态的性能差异.

#### 3.1.1　数据集描述

我们使用一个公开的大规模数据集[20]进行实验评估. 该数据集包含100位用户数据. 记录了用户在执行会话过程中加速度计,陀螺仪及磁力计等运动传感器读数和触控数据. 实验中将用户自己数据作为合法用户数据,其他用户数据作为非法用户数据,混合划分训练集和测试集,划分比例为7:3.

#### 3.1.2　评估指标

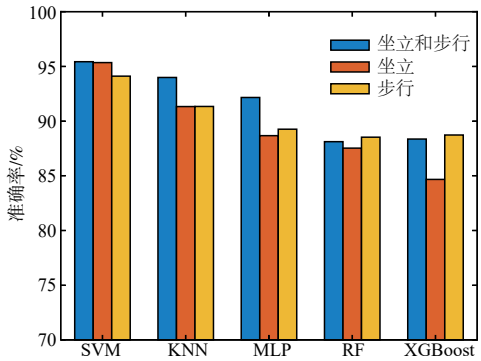
在实验中,将分类准确率作为判断分类器分类性能的指标,准确率指包括合法用户和冒用用户在内的所有数据中准确识别的比率,准确率高的分类器分类能力好. 在针对两种行为的身份认证实验中,采用EER作为评估标准,EER指调整阈值后,FRR等于FAR时的值,其中FRR为将合法用户识别为非法用户的概率,FAR为非法用户识别为合法用户的概率. 除此之外,我们使用了受试者工作特征(Receiver Operating Characteristic, ROC)曲线可视化模型认证能力.

#### 3.1.3　单模态认证评估

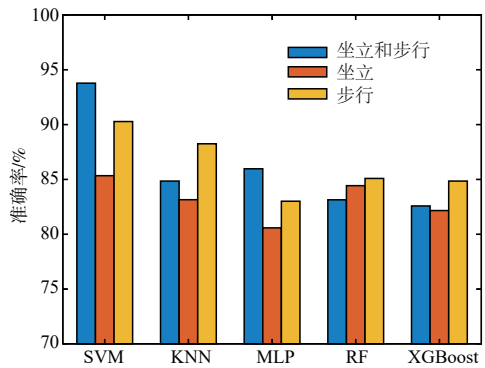
表2展示了触屏时触控传感器行为与运动传感器行为在用户坐立和步行两种运动状态以及不区分运动状态下的认证准确率,表中的每一行显示了在一种分类器下的结果. 从表中可以观察到,SVM在所有的情况下都比其他四个分类器的认证能力强,在不区分运动状态的情况下,SVM在触控传感器行为的准确率达到了95.43%,对于运动传感器行为的准确率达到了93.78%,相对于RF在触控传感器行为下的88.12%,以及XGBoost在运动传感器行为下的82.58%,SVM表现出了优越的分类能力. 除此之外,KNN和MLP在运动传感器行为上也表现出了较佳的性能,准确率分别为93.99%和92.16%. 我们猜测由于XGBoost适用于大规模训练数据的场景,因而在本次实验中,训练数据仅有数百条下,效果欠佳仅为82.58%.

表2中另外的观察是触控传感器行为比运动传感器行为的认证准确率高,最小的差距为2%,最大为6%,说明触控传感器行为在用户间更具有判别力. 除此之外,图4对比了触屏时触控传感器行为和运动传感器行为在不同分类器下不同运动状态准确率. 从图中我们可以看出,触控传感器行为在不同的运动状态下

相对比较稳定,而运动传感器行为在步行运动状态下的准确率明显高于坐着时的准确率.




(a) 触控传感器行为




(b) 运动传感器行为

图4 两种行为在不同分类器下不同运动状态准确率对比图

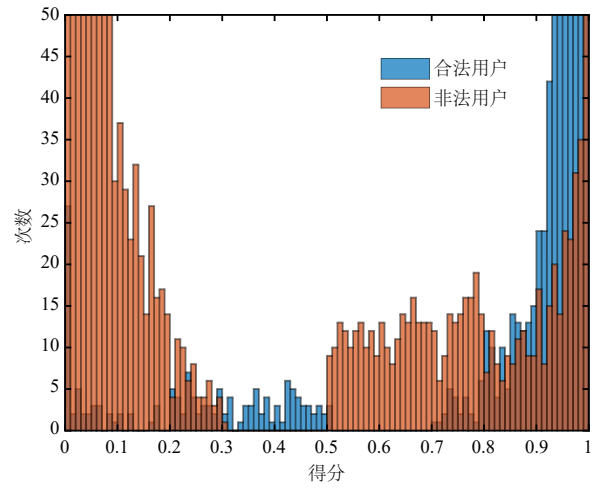
**表2 坐立和步行以及不区分运动状态情况下,触屏时触控传感器行为和运动传感器行为在不同分类器下认证的准确率**

| | 坐立 | | 步行 | | 不区分运动状态 | |
|---|---|---|---|---|---|---|
| | 触控传感器 | 运动传感器 | 触控传感器 | 运动传感器 | 触控传感器 | 运动传感器 |
| SVM | 95.35% | 85.34% | 94.11% | 90.28% | 95.41% | 93.78% |
| KNN | 91.33% | 83.15% | 91.34% | 88.25% | 93.99% | 84.85% |
| MLP | 88.67% | 80.58% | 89.26% | 83.01% | 92.16% | 85.97% |
| RF | 87.53% | 84.43% | 88.53% | 85.09% | 88.12% | 83.14% |
| XGBoost | 84.67% | 82.16% | 88.73% | 84.85% | 88.36% | 82.58% |

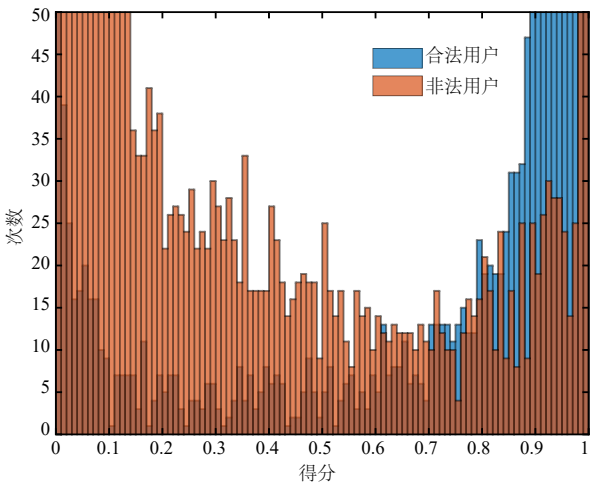
### 3.1.4 多模态认证评估

我们使用上述实验所有分类器中表现最好的SVM进行双模态认证实验. 图5展示了触屏时触控传感器行为和运动传感器行为的合法用户和非法用户决策分数分布. 可以看出,触控传感器行为认证的合法用户和非法用户的得分的分离程度更大,因而触控传感器行为在计算融合决策分数时占据更高的权重,根据融合公式最终计算的权重比为0.52:0.48.

图6展示了触屏时触控传感器行为和运动传感器




(a) 触控传感器行为




(b) 运动传感器行为

图5 两种传感器行为的合法用户和非法用户决策得分分布

行为以及它们的融合之后的ROC. 可以看出,融合之后的ROC略好于触控传感器行为,EER从触控传感器行为的3.467%降低到了3.08%,其准确率从95.43%上升到了97.19%. 除此之外,运动传感器行为的EER只有5.763%,两种行为融合之后EER降低了2.7%. 图7显示了随着触屏操作次数增加,认证准确率也随之提高. 同时,也可以看出,两种行为的融合均优于单行为的认证效果.

## 3.2 自适应模型评估

### 3.2.1 可行性分析

我们对用户手机使用历史数据进行了持续一周的收集,对于每一个用户,当他/她使用一个应用程序时,我们记录当前使用环境的上下文信息,包括地理位置和当前使用的应用程序名称,同时要求每位用户根据自己的需求将所有使用的应用程序分为不重要、重要、

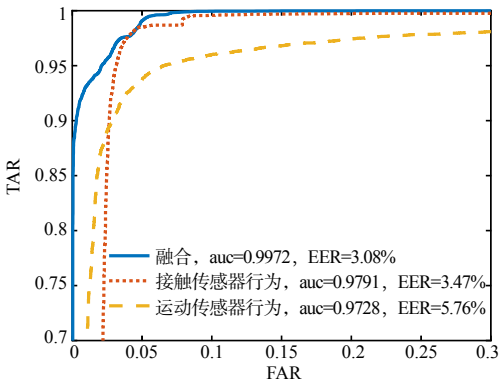



图6　单模态和多模融合ROC曲线对比

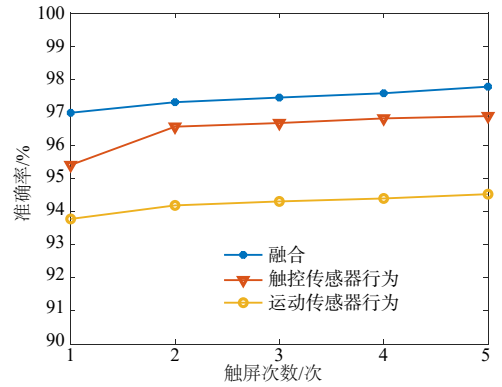



图7　多次触屏操作下单模态和多模态准确率对比

极其重要三类.

针对获取的数据,我们首先统计了用户的位置轨迹以及应用程序的使用情况. 图8展示了其中三位用户在使用手机时地理位置的分布情况. 从图中可看出,用户1和用户2近80%的时间在地点1和地点2,据调查发现这两个地点分别是居住的地方(家或者宿舍)和学习工作的地方,而用户3地理位置分布比较均匀,这是由于在采集数据的一周内,用户3由于工作需要在外出差,因此居住地和工作的地点不属于自己日常生活的一部分,但是前两个地点也占40%. 表3展示了相应的三位用户使用应用程序的频次分布. 从表中可以了

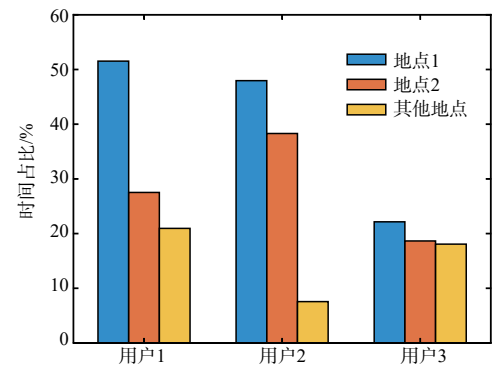



图8三个不同用户使用手机地理位置统计

**表3　用户使用最多的十个应用程序以及它们占比**

| 用户1 | 占比 | 用户2 | 占比 | 用户3 | 占比 |
|---|---|---|---|---|---|
| TIM | 30.72% | 微信 | 42.87% | TIM | 38.12% |
| 微信 | 23.37% | 微博 | 12.09% | 微信 | 31.95% |
| 微博 | 7.83% | 抖音 | 5.72% | 哔哩哔哩 | 10.76% |
| 哔哩哔哩 | 6.05% | 淘宝 | 5.48% | 知乎 | 3.60% |
| 计算器 | 4.27% | 浏览器 | 4.43% | 支付宝 | 3.35% |
| 支付宝 | 4.27% | 腾讯视频 | 3.87% | 淘宝 | 2.48% |
| 浏览器 | 3.08% | QQ音乐 | 3.79% | TFT | 2.24% |
| 淘宝 | 3.08% | QQ | 3.71% | 浏览器 | 1.61% |
| 知乎 | 2.97% | 得物 | 2.82% | 高德地图 | 1.28% |
| 闹钟 | 2.37% | 小红书 | 1.93% | U加速器 | 0.99% |

解到,每个用户平均每周使用前5个应用程序占比77%. 根据分析,我们可以看出,用户趋向于在熟悉的地方以及经常使用少数固定的应用程序,因此我们采用这两种上下文特征来表征上下文安全水平是可行且可靠的.

### 3.2.2　自适应模型评估

通过4.1.4节的实验,我们可以发现,触屏时触控传感器行为和运动传感器行为在融合之后可以提高安全性的同时提升认证能力. 但是,双模态融合在数据收集和处理等过程也会带来额外的能耗开销.

由于触控传感器行为在触屏操作过程中发生,因此它的能量消耗是不可避免的,而运动传感器行为属于额外的能耗. 因此,我们使用性能与功耗测试工具Trepn Profile来监视不同手机下运动传感器行为在数据收集和特征提取过程中电池消耗情况,我们持续运行了数据收集和特征提取程序3个小时进行测试. 该程序可以收集包括加速度计、陀螺仪以及磁力计在内的运动传感器的三维数据并进行特征提取,数据采样频率为100 Hz. 测试结果如表4所示,从表中可以看出,持续地对运动传感器进行数据收集和处理是一项耗能的工作.

**表4　不同手机下运动传感器在3个小时的数据收集过程中电池消耗情况(单位:mAh)**

| 编号 | 手机型号 | 电池消耗/总电量mAh |
|---|---|---|
| 1 | 华为PIC-AL00 | 354/2950 |
| 2 | OPPO R17 | 525/3500 |
| 3 | 小米8 SE | 655.2/3120 |

综合4.1.3节与4.1.4节实验,可以发现,相比于运动传感器行为,触控传感器行为的认证能力更好,不同运动状态下的鲁棒性更强,且带来的额外开销更小. 根据我们在第3节提出的自适应模型,可以仅在需要高强度的持续认证时同时使用两种行为的融合,而在一般情况下单独使用基于单模态的持续认证以达到节省能耗的目的,可采用触控传感器行为作为此情况下的认

证手段.

根据收集的数据,我们对提出的自适应系统进行评估. 实验中,为了计算式(6),我们根据用户的划分,将不重要的应用程序的保护程度$v$值设置为1,重要的应用程序$v$值设置为2,极其重要的应用程序$v$值设置为3. 阈值选择为0.6. 本文考虑的是低耗能的基于触控传感器行为的持续认证和高耗能但更安全的基于触控传感器行为和运动传感器行为的持续认证. 根据收集的数据进行实验后表明,采用了自适应系统之后,所有用户平均54.85%的时间不需要采用高强度的多模融合持续认证.

### 3.3 相关文献对比评估

表5列出了本文方案与相关文献的触屏认证方案对比细节. 从表中可以看出,文献[4]为基于触控传感器的单模行为认证,其不需要额外的能耗来源,但其认证能力相比于本文方案中双模融合较差;文献[6]为基于运动传感器的单模行为认证,其不仅认证能力低,而且还忽略了能耗问题;而文献[7]是两种行为的融合认证,但是该文献的认证能力最低,并且未采用自适应手段来应对多模认证带来的系统复杂性和能耗的增加. 综合考虑下,本文方案具有较好的适应性,更有利于触屏持续认证系统的推广应用.

**表5 方案对比(能耗占比为能耗来源在整个认证过程的时间占比)**

| 方案 | 触屏行为 | 认证性能(EER) | 能耗来源 | 是否自适应 | 能耗占比 |
|---|---|---|---|---|---|
| 本文 | 触控传感器行为 | 3.47% | 无 | 否 | 0% |
| | 运动传感器行为 | 5.76% | 运动传感器 | 否 | 100% |
| | 自适应融合 | 3.08% | 运动传感器 | 是 | 45.15% |
| 文献[4] | 触控传感器行为 | 4% | 无 | 否 | 0% |
| 文献[6] | 运动传感器行为 | 4.71% | 运动传感器 | 否 | 100% |
| 文献[7] | 融合 | 7.16%(行走)<br>10.05%(坐着) | 运动传感器 | 否 | 100% |

## 4 结论

针对行为认证易受外界环境影响且可能遭受模仿攻击和统计攻击的问题,本文首先融合触屏时触控传感器行为和运动传感器行为进行双模态认证,以此来提高对外界环境的鲁棒性以及增加攻击难度来增强安全性. 另一方面考虑到双模态认证系统相对于单模态认证系统的复杂性以及触屏时运动传感器行为持续对包括加速度计、陀螺仪和磁力计在内的传感器进行数据采集和处理分析带来大量的CPU资源和电量消耗. 本文提出了一个自适应触屏持续认证方案,可以根据上下文自适应地选择认证强度,通过避免使用触屏时运动传感器行为认证达到降低认证系统复杂性以及能耗的目的,实验表明该方案在提供足够设备安全性的同时使能耗降低50%以上.

**参考文献**


[1] PATEL V M, CHELLAPPA R, CHANDRA D, et al. Continuous user authentication on mobile devices: recent progress and remaining challenges[J]. IEEE Signal Processing Magazine, 2016, 33(4): 49-61.

[2] ABUHAMAD M, ABUSNAINA A, NYANG D H, et al. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: a survey[J]. IEEE Internet of Things Journal, 2020, 8(1): 65-84.

[3] 徐国愚,苗许娜,张俊峰,等. 面向移动终端的隐式身份认证机制综述[J]. 计算机工程与应用, 2018, 54(6): 19-25.
XU Guoyu, MIAO Xuna, ZHANG Junfeng, et al. Review of implicit authentication for mobile devices[J]. Computer Engineering and Applications, 2018, 54(06): 19-25.

[4] FRANK M, BIEDERT R, MA E, et al. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication[J]. IEEE Transactions on Information Forensics and Security, 2012, 8(1): 136 -148.

[5] FIERREZ J, POZO A, MARTINEZ-DIAZ M, et al. Benchmarking touchscreen biometrics for mobile authentication [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(11): 2720-2733.

[6] SHEN C, LI Y, CHEN Y, et al. Performance analysis of multi-motion sensor behavior for active smartphone authentication[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(1): 48-62.

[7] SITOVÁ Z, ŠEDĚNKA J, YANG Q, et al. HMOG: new behavioral biometric features for continuous authentication of smartphone users[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(5): 877-892.

[8] CHENG B, ZHANG L, LI X Y, et al. SilentSense: silent user identification via touch and movement behavioral biometrics[C]//Proceedings of the 19th Annual International Conference on Mobile Computing Networking MobiCom. New York: Association for Computing Machinery, 2013:

187-190.
[9] LEE W, LEE R B. Multi-sensor authentication to improve smartphone security[C]//2015 International Conference on Information Systems Security and Privacy. France: IEEE, 2015: 1-11.
[10] ROSS A, POH N. Multibiometric Systems: Overview, Case Studies and Open Issues[M]. Germany: Springer, 2014: 273-192.
[11] PHOHA V V, SERWADDA A. When kids' toys breach mobile phone security[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. Berlin: Association for Computing Machinery, 2013: 559-610.
[12] EBERZ S, LOVISOTTO G, PATANÈ A, et al. When your fitness tracker betrays you: quantifying the predictability of biometric features across contexts[C]//2018 IEEE Symposium on Security and Privacy. San Francisco: IEEE, 2018: 889-905.
[13] NAMBIAR A, BERNARDINO A, NASCIMENTO J C, et al. Context-aware person re-identification in the wild via fusion of gait and anthropometric features[C]//IEEE International Conference on Automatic Face & Gesture Recognition. Washington: IEEE, 2017: 973-980.
[14] SANDIP K, VIJAY K, et al. Multibiometric fusion strategy and its applications: A review[J]. Information Fusion, 2019, 49(1566-2535): 174-204.
[15] FRIDMAN L, WEBER S, GREENSTADT R, et al. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location[J]. IEEE Systems Journal, 2017, 11(2): 513-521.
[16] MAHBUB U, KOMULAINEN J, FERREIRA D, et al. Continuous authentication of smartphones based on application usage[J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019, 1(3): 165-180.
[17] SHEMA A, ACUNA D E. Show me your APP usage and I will tell who your close friends are: predicting user's context from simple cellphone activity[C]//CHI Conference Extended Abstracts on Human Factors in Computing Systems. Denver Colorado: Association for Computing Machinery, 2017: 2929-2935.
[18] CRANSHAW J, TOCH E, HONG J I, et al. Bridging the gap between physical location and online social networks [C]//Ubiquitous Computing, 12th International Conference. Copenhagen: Social Science Research Network, 2010: 26 -29.
[19] STANLEY F C, JOSHUA G. An empirical study of smoothing techniques for language modeling[J]. Computer Speech & Language, 1999, 13(4): 359-394.
[20] QING Y, GE P, DAVID T, et al. A multimodal data set for evaluating continuous authentication performance in smartphones[C]//Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems. New York: Association for Computing Machinery, 2014: 358-359.

## 作者简介

**姜　奇**　男,1983年9月出生于安徽省全椒县. 现为西安电子科技大学网络与信息安全学院教授、博士生导师. 主要研究方向为密码协议,物联网安全. 在国内外发表学术论文80余篇.
E-mail: jiangqixdu@gmail.com

**文　悦**　女,1997年7月出生于陕西省铜川市. 现为西安电子科技大学网络与信息安全学院研究生,主要研究方向为生物认证.
E-mail: wen2586645609@163.com

**张瑞杰**　女,1984年生于河南郑州,博士,战略支援部队信息工程大学三院讲师. 主要研究方向为人工智能、网络信息防御等.
E-mail: rjz_wonder@163.com

**魏福山**　男,1983年生于甘肃省武威市. 现为战略支援部队信息工程大学四院副教授,博士生导师. 主要研究方向为安全协议设计与分析.
E-mail: weifs831020@163.com

**马建峰**　男,1963年生于陕西西安. 西安电子科技大学网络与信息安全学院教授,博士生导师. 研究方向为密码学、计算机网络与信息安全.
E-mail: jfma@mail.xidian.edu.cn