TouchAuth：基于触屏行为的隐式持续用户身份认证机制

马璐萍[1,2], 朱大立[1,2], 张顺亮[1,2], 马宇晨[1,2], 冯维淼[1,2], 彭淑敏[3], 张珠君[1,2]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]中国科学院大学网络空间安全学院 北京 中国 100049
[3]郑州大学信息工程学院 郑州 中国 450000

摘要 随着移动互联网的日益普及, 越来越多的用户将大量敏感信息存入移动终端, 保护移动终端中的隐私数据和敏感信息不被他人非法查看已成为亟待解决的问题。用户身份认证机制通常被用于移动终端中的隐私信息保护, 但传统的身份验证方法在用户通过初始身份验证后不能提供持续的保护从而导致隐私泄露。为解决这一问题, 大量基于触屏行为的用户身份认证机制被提出来, 然而这些机制通常具有如下局限性—身份认证效果通常局限于某一类(几类)场景或依赖于会话内操作稀疏程度。为解决如上问题, 本文提出了一种支持多属性关联的特征采样方法及基于用户触屏行为驱动的隐式持续身份认证机制 TouchAuth。TouchAuth 对用户触屏行为数据进行采样以提取用户行为特征信息, 然后采用典型的机器学习方法判断用户触屏行为的合法性。为提高 TouchAuth 的稳定性和准确性, 我们引入了决策步长机制, 通过综合判断决策步长内多个触屏行为的合法性来确定用户合法性。基于公开数据集合的大量实验结果表明: 攻击者仅完成 7 次本文定义的触屏行为就可以被 TouchAuth 检测到, 平均 *EER* 为 11%, 这优于现有身份认证机制。TouchAuth 克服了以往基于用户触屏行为进行身份认证的机制局限于某一类场景或某一类(几类)应用程序, 以及会话内操作稀疏时身份认证效果无法保证的缺陷。

关键词 隐私保护; 隐式持续身份认证; 触屏行为
中图法分类号 0000 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.08.10

TouchAuth: An Implicit Continuous User Identity Authentication Mechanism based on Touch Screen Behavior

MA Luping[1,2], ZHU Dali[1,2], ZHANG Shunliang[1,2], MA Yuchen[1,2], Feng Weimiao[1,2], PENG Shumin[3], ZHANG Zhujun[1,2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China
[3]School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

Abstract With the increasing popularity of mobile internet, an increasing amount of sensitive data are stored on mobile terminals. Thus, protecting a large amount of private data and sensitive information in mobile terminals from being illegally viewed by others has become an urgent problem to be solved. A user identification authentication mechanism is usually employed for privacy information protection in mobile terminals. However, traditional authentication methods cannot provide continuous protection after the user passes the initial authentication, which leads to privacy leakage. To address this issue, identity authentication schemes have been proposed based on user touchscreen behavior, but their application scenarios often have limitations—the authentication efficiency is often limited to a certain scenario or application, or the authentication efficiency cannot be guaranteed when the operations in the session are sparse. Hence, this paper proposes TouchAuth, a feature sampling method that supports multi-attribute association and an implicit continuous identity authentication mechanism based on user touch screen behavior to overcome the above issues and achieve real-time identity authentication when using mobile terminals. Based on the proposed feature sampling method, TouchAuth samples the user's touch screen behavior data and judges its legitimacy using typical machine learning approaches. Additionally, we introduce a decision-step mechanism to improve the stability and accuracy of TouchAuth, which determines the users' legitimacy by comprehensively judging the legitimacy of multiple touchscreen behaviors in the decision steps. Experimental results on a public dataset demonstrate that TouchAuth can detect the attacker with an average *EER* of 11%, based on data from seven touches, as defined in this paper. Moreover, TouchAuth overcomes the problem of authentication efficiency

通讯作者： 朱大立, 博士,正研级高级工程师, Email: zhudali@iie.ac.cn。
本课题得到国家重点研发计划(No. 2019YFB1005200)资助。
收稿日期: 2021-01-26; 修改日期: 2021-04-27; 定稿日期: 2023-08-09

being limited to a certain scenario or application and not guaranteed when the session operations are sparse.

Key words privacy protection; implicit continuous identity authentication; touch screen behavior

1 引言

IDC 预计到 2023 年智能手机市场中的终端数量将达到 14.89 亿部[1]。随着移动终端功能日益丰富, 越来越多的隐私信息(比如联系人信息、照片等)被用户存储在移动终端上。文献[2]表明, 大约有92.8%的用户倾向于将个人信息存储在移动设备中。防止移动终端中的信息被他人非法查看已成为防止用户隐私泄露的重要方面。

目前, 移动设备主要在用户解锁屏幕时进行显式身份认证, 认证方式主要采用基于知识或生物特征的方案。基于知识的方法依赖于用户的知识, 即用户必须提供某些信息(例如: 个人识别码(PIN)、图形密码或图片手势)来证明合法身份。基于生物特征的方法是基于如面部[3]、指纹[4-5]、虹膜[6]等生物特征进行身份认证。

如上身份认证方案有以下共同的缺点: 无法提供持续、隐式和透明的身份验证。如果密码被泄露, 或者用户在移动终端上的初始认证通过后没有足够的警惕性, 则未经授权的个人可能非法地访问移动终端上存储的信息。

因此, 需要一种可以在用户使用移动终端的过程中持续、隐式判断用户身份合法性的技术作为对如上所述认证技术(使用基于知识或生物特征的显示认证)的补充(这些认证技术通常被称为“透明的、连续的、隐式的、主动的、被动的、非侵入的、不可观察的、自适应的、不引人注目的和渐进的[7]”)。其中隐式、持续身份认证技术的主要任务是检测任何试图非法查看移动终端信息的攻击者。因此, 应该协同使用显式和隐式的认证方法以确保移动终端中信息不被非法查看。

调查[8]表明, 90%的研究参与者倾向于基于行为生物特征的透明认证。调查[9]表明, 尽管存在局限性, 用户还是接受了使用这种非侵入性方案进行身份验证。主动认证研究得到了广泛的关注[10], 大量的隐式、持续身份认证技术被提出, 但是已有的解决方案在保护用户移动终端上的隐私数据不被非法查看方面都存在一些缺陷, 主要可以分为如下几个方面:

1) 无法确保用户在触屏查看移动终端信息时进行隐式、持续的身份认证;

基于击键的隐式身份认证方法[11-13]仅在用户与键盘交互时才起作用。文献[14]基于用户拿起手机的动作隐式判断用户身份。如果用户未做出如上方案中用于判断用户身份的动作, 仅触屏查看手机内容时, 则较难判别用户身份。文献[15]在满足手机屏幕已打开且当前活动的应用程序与上一个应用程序不同时, 会持续采集加速度传感器、陀螺仪传感器和重力传感器 3 秒钟, 使用采集的数据识别用户身份。如果不满足如上鉴别身份的条件, 则不会采集传感器数据进行身份鉴别, 此时非法用户就可以查看手机上内容。

2) 涉及过多的用户敏感隐私数据;

基于手机使用行为进行身份鉴别的方案[16-17]需要获取用户生活隐私数据, 比如: 浏览记录、位置信息等。

3) 无法避免在用户未触屏查看移动终端时的无效身份鉴别;

文献[18]通过加速度传感器和陀螺仪提取步态生物特征进行身份认证。文献[19]使用加速计、陀螺仪等捕捉用户的行为模式进行身份验证。这些机制存在用户未触屏查看移动终端时进行身份认证的情况。调查[20]显示在美国, 智能手机用户每天花在移动应用上的时间约为 2 小时 51 分钟。研究[21]表明, 用户在连续使用手机之间可能有很长的空闲时间。在此期间, 身份验证是一个冗余操作, 因为没有任何应用程序在前台运行。

为解决如上问题, 需要寻找更加适合保护移动终端上信息不被非法查看的身份认证机制及所需的用户行为数据:

1) 用户查看移动终端时通常需要触屏操作, 为防止移动终端上的信息被非法查看, 最合适的身份认证数据是触屏行为数据;

2) 触屏行为数据不涉及用户浏览记录等用户敏感信息, 因此需要研究仅使用触屏行为数据的身份认证机制;

3) 如果身份认证机制是在用户触屏行为驱动下(用户有触屏行为时)判断用户身份, 则可以有效避免用户未查看移动终端时的无效身份认证。

但是已有的基于触屏行为的隐式持续身份认证机制有如下几方面的缺陷:

1) 身份认证效果局限于某一类场景或某一类(几类)应用程序, 如果用户在非指定应用或场景中使用移动终端则无法保证身份认证效果;

比如, 文献[22]为 Android 平台上可用的不同类型的输入控件创建基本分类器, 并将它们组合

到一个集成分类器中, 以验证和识别用户。此方案需要每个用户在使用应用程序的会话期间与每种类型输入控件的 15～20 个实例进行交互, 此方案的缺陷是对身份认证的场景进行了限制。文献[23]引入了一种基于模糊分类器的连续认证系统, 该框架旨在保护移动银行应用程序的安全。文献[24]基于从网络浏览手势中提取出来的 21 个特征实现了一种认证方案 TouchWB, 用于在网络浏览应用中识别用户身份。文献[23-24]的身份认证效果仅局限于特定应用程序。文献[25]为每个正在运行的应用程序维护不同的手势模板, 并执行自适应分类来进行用户身份识别。此方案在用户操作未建立身份认证模板的应用程序时无法保证身份认证效果。

2) 无法保证会话内操作稀疏时的身份认证效果;

文献[24,32]中用户每操作移动终端 10 分钟作为一个会话, 以会话为单位提取触屏行为特征, 并基于此特征对用户进行身份鉴别。这些方案的缺陷是如果攻击者每次操作时间间隔较大, 10 分钟的会话期间采集到的攻击者操作较少导致无法提取足够的特征数据, 则影响认证效果。文献[22-23]中用户每完成一组指定的任务作为一个会话, 并以一部分会话作为训练数据建立身份认证模型, 基于此模型识别用户身份。如果攻击者在会话期间的行为未覆盖大部分指定任务, 则可能影响认证效果。

为解决如上问题, 需要研究一种基于触屏行为的身份认证机制。因此本文提出 TouchAuth, 一种基于用户触屏行为驱动的隐式持续身份认证机制。本文的贡献主要分为如下几个方面:

1) 提出一种支持多属性关联学习的提取用户触屏行为特征的采样方法;

2) 提出一种基于触屏行为驱动的身份认证机制 TouchAuth, 此机制具备如下优点:

- 身份认证效果不局限于某一类场景或某一类(几类)应用程序;
- 可避免用户未查看移动终端时的无效身份鉴别;
- 可在用户触屏查看移动终端信息时进行隐式、持续的身份认证;
- 可以避免会话内操作稀疏对身份认证效果的影响。

3) 在公开数据集合 UMDAA-02[26]上的实验证明: 攻击者仅完成 7 次本文定义的触屏行为就可以被 TouchAuth 检测到。TouchAuth 的平均 *F*1-*score* 为 88.45%, 平均 *FAR* 为 10.1%, 平均 *FRR* 为 9.95%, 平均 *EER* 为 11%。与已有的两种机制[27-28]相比, 本文提出的身份认证机制 *EER* 分别下降了 11%和 20.93%。

本文剩余部分的组织结构如下: 第 2 节介绍了本文的研究背景和相关工作。第 3 节介绍了威胁模型。第 4 节介绍本文所提出的 TouchAuth 的原理。第 5 节对实验结果进行了分析讨论。第 6 节总结了本文工作。

2 背景及相关工作

2.1 基于触屏行为的身份认证机制

本节中, 我们对现有的基于触屏数据进行身份认证的典型方法进行了回顾。在简要介绍这些方案的同时我们在表 1 中使用以下标准对这些方案进行了比较:

1) “使用方法”列出了该方案的分类方法;

2) “数据大小”表示实验阶段的参与者或样本数量;

3) “数据集合是否可控”表示实验采用的数据集合是否可控(可控是指自己招募的实验志愿者, 而非使用公开数据集);

4) “效果”表示此方案的实验效果。

文献[29]介绍了一种基于 Dynamic Time Warping 的多点触摸手势认证技术。在 34 名参与者使用单一手势的情况下, 该方案获得了 90%的准确率, 使用按顺序执行的多个手势可以显著提高准确率。但是这种身份认证方式的缺点是需要用户做出特定的手势。

文献[30]介绍了一种旨在增强 Android 登录过程的隐式生物认证方法。作者开发了一个 Android 应用程序, 它有四个不同的解锁屏幕和密码模式, 用于收集用户数据以评估方案效果。该方案采用 Dynamic Time Warping 方法来区分不同的参与者。实验结果表明, 该方案平均准确率为 77%, 但是这种方案仅用于对登录过程的安全增强, 无法进行隐式持续身份认证。

文献[31]收集 41 名实验参与者完成预先设定任务过程中的触屏行为, 对这些触屏行为提取 30 种触屏行为特征, 并采用 KNN(K-Nearest Neighbor)和高斯 RBF 核支持向量机(Gaussian RBF Kernel Support Vector Machine)进行身份认证。实验证明, 此方案的 *EER* 在 0%～4%之间。这种方案的缺点是: 身份认证效果仅局限于作者编写的用于引导实验参与者执行特定任务以采集触屏行为的应用程序。

文献[33]提取手指触屏轨迹以及接触区域形状, 在仅仅 5 次触屏之后, 或者平均 12.6 秒就可以正确区分主要用户和其他 14 个已知用户中的任何一个, 但是这种方案的效果是区分已知用户。

表 1 相关工作

Table 1 Related Work

	数据大小	使用方法	数据集合是否不可控	效果
文献[29]	34 人	Dynamic Time Warping	否	单手势时 *EER* 为 10%, 双手势时 *EER* 为 5%
文献[30]	48 人	Dynamic Time Warping	否	平均准确率 77%
文献[31]	41 人	k-Nearest Neighbor, Gaussian RBF Kernel Support Vector Machine	否	*EER* 介于 0%和 4%之间
文献[32]	20 人	J48 tree, Naive Bayes 、Kstar、Radial-Basis Function Networks、Back Propagation Neural Network	否	RBFN 的平均 *EER* 为 7.8%
文献[23]	22 人	fuzzy classifier	否	平均 *EER* 为 11.5%
文献[25]	123 人	结合了 One Nearest Neighbor 和 Dynamic Time Warping	否	准确率为 90%
文献[33]	14 人	Artificial Neural Network 和 Support Vector Machines	否	准确率 99.9%
文献[34]	15009 个手势样本和 10054 个签名样本	Support Vector Distribution Estimation	否	手势的平均 *EER* 为 0.5%, 签名的平均 *EER* 为 0.52%
文献[35]	3203 个合法 PIN 和 4655 个伪造样本	Dynamic Time Warping、K-Nearest Neighbor	否	平均 *EER* 为 4.8%
文献[22]	42 人	Support Vector Machines	否	平均 *EER* 为 7%, 平均准确率为 93%
文献[24]	48 人	Particle Swarm Optimization—Radial Basis Function Networks	否	平均 *EER* 为 2.4%

文献[34]根据用户在触摸屏上执行特定操作(手势或签名)的行为特征来对用户进行身份验证, 并采集了 15009 个手势样本和 10054 个签名样本进行实验。实验结果表明, 在 25 个训练样本的情况下, 此方案基于手势识别身份的平均 *EER* 为 0.5%, 基于单次签名识别身份的平均 *EER* 为 0.52%。这种方案的缺点是无法实现隐式持续身份认证。

文献[35]提出的 DRAW-A-PIN, 要求用户在触摸屏上绘制一个 PIN。该方案采用了 PIN 内容分析器和绘图行为分析器来识别非法用户。但是这种方案是对于单次显式身份认证的安全增强, 无法实现隐式、持续身份认证。

文献[22-25]提出的身份认证效果局限于某一类场景或某一类(几类)应用程序。文献[22-24,32]提出的方案无法保证会话内操作稀疏时的身份认证效果(已在引言中介绍)。

从表 1 中可看出, 所列方案中使用的实验数据都是可控数据, 本文所采用的实验数据包含不可控数据(公开数据集)和可控数据。

2.2 公共数据集

尽管基于触屏数据的身份认证方案需要大量用户触屏行为数据, 但是公开可用并且符合本文所需特征的数据集却很少。

数据集[36]收集了 218 名匿名参与者大约 6 个月的时间里使用手机的如下数据: 用户当前使用的应用程序、用户安装\删除或更新的应用程序、应用程序请求的权限、应用服务连接信息(例如, 服务器 IP 地址、用于连接的端口等)、在建立网络连接时的用户位置等。

数据集[37]包括 25 个用户在几天至一年的时间段内使用 iPhone 3GS 设备的数据, 包括: 应用程序使用情况、网络使用情况、GPS 数据、电池使用情况和加速度计数据等。

但是如上数据集都不满足本文所需的触屏行为数据需求。本文采用的公共数据集是马里兰大学的主动认证数据集 UMDAA-02[26]。此数据集是专门为评估主动身份验证系统而设计的。其数据来自 45 名志愿者两个月的日常生活中使用 Nexus5 手机的数据。数据采集应用程序完全在后台运行, 采集的数据包括触屏行为数据 、前置摄像头、陀螺仪、加速度计、磁强计、光传感器、GPS、蓝牙、Wi-Fi、温度传感器等数据。

3 威胁模型

本文考虑这样一个攻击场景: 攻击者可以拿到合法用户的移动终端, 并且已经拥有密码(例如 PIN 码或指纹)来解锁设备。因此, 攻击者可以查看移动终端中存储的敏感信息, 比如: 查看短信、微信聊天记录、

通讯录等。本文的目标是通过分析用户使用移动终端的触屏行为习惯, 开发基于用户触屏行为的持续、隐式身份认证机制。在用户查看移动终端时, 本机制基于触屏行为数据对用户身份的合法性进行判断。

4 TouchAuth 模型

方案[38]表明用户在使用移动设备时倾向于形成独特的行为模式, 这些行为模式可用于身份验证任务。方案[39]表明不同的用户会产生不同程度的姿势和动作变化, 表现出独特的行为特征。本文提出了一种基于触屏行为驱动的持续、隐式身份认证机制—TouchAuth。TouchAuth 提取用户触屏行为特征后, 使用特征数据判断用户身份的合法性。

图 1 展示了 TouchAuth 的架构图, 主要包含三个模块: 1)数据处理模块; 2)行为分类器; 3)身份决策器。

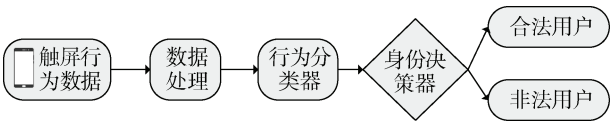

图 1 TouchAuth 架构图

Figure 1 TouchAuth architecture

数据处理模块: 对用户触屏行为数据进行采样, 并进行归一化处理。

行为分类器: 从用户历史触屏行为数据中学习用户触屏行为规律, 通过度量当前行为与历史行为的差异, 来确定当前行为的合法性。

身份决策器: 只凭单一动作不足以判断用户身份。为了提高 TouchAuth 的认证准确度和稳定性, 我们引入决策步长机制, 综合决策步长内所有动作的合法性确定用户身份。

下文介绍 TouchAuth 的数据定义、身份识别机制依据、采样方式以及行为分类器、身份决策器的原理。

4.1 数据定义

在阐述 TouchAuth 技术原理前, 我们首先给出 TouchAuth 涉及的相关数据的定义。具体定义如下:

定义 1: 用户使用移动终端时, 从用户手部按压下屏幕到手部抬起的动作, 在本文中被定义为一次触屏行 N_i, 用户的 p 次触屏行为集合为 $\{N_0,\ldots,N_i,\ldots,N_p\}$。

Android 操作系统通常可以获取用户触屏行为的位置坐标(在移动终端屏幕上的位置)、压力及动作类型(按下或抬起等)。因此本文对 Android 操作系统采集到的用户触屏行为数据进行如下定义。

定义 2: 一次触屏行为 N_i 可以被 Android 操作系统采集为一系列的数据序列 $\left\{N_i^{(0)},N_i^{(1)},\ldots,N_i^{(n)}\right\}$。其中 $N_i^{(n)}$ 为 Android 操作系统采集到的触屏行为 N_i 的第 n+1 个点的数据。

定义 3: $N_i^{(n)}=\langle TI_{i(n)},X_{i(n)},Y_{i(n)},TY_{i(n)},P_{i(n)}\rangle$, 其中每一项的具体含义如下:

1) 移动终端屏幕的长和宽作为 X, Y 坐标轴, $\left(X_{i(n)},Y_{i(n)}\right)$ 代表 $N_i^{(n)}$ 在 X, Y 坐标轴上的位置;

2) $TI_{i(n)}$ 代表 $N_i^{(n)}$ 的触屏停留时间, 即 N_i^{n+1} 与 N_i^n 的时间差;

3) $TY_{i(n)}$ 代表 $N_i^{(n)}$ 的触屏动作类型, 包括按下动作, 抬起或滑动动作;

4) $P_{i(n)}$ 代表 $N_i^{(n)}$ 的压力大小。

4.2 TouchAuth 身份识别机制依据

4.2.1 身份识别方案选择

为避免 TouchAuth 具有已有基于触屏行为的身份认证机制中存在的缺陷, 我们分析了导致这些缺陷的原因:

1) 已有的方案身份认证效果局限于某一类场景或某一类(几类)应用程序的主要原因是这些机制对身份认证的场景进行了限定, 具体而言:

- 身份认证的过程中需要用户的行为满足某些规则(比如: 文献[22])才能保证身份认证效果;
- 在训练用户身份认证模板时的输入数据局限于从某一类应用程序中提取出的用户行为, 导致该模板的身份认证效果仅局限于此类应用程序(比如文献[23-25])。

为避免 TouchAuth 存在如上缺陷, 本文的身份认证机制具备如下特点:

- TouchAuth 没有对用户的行为进行限制, 其用户身份认证场景为: 用户在无任何限制的情况下使用移动终端;
- TouchAuth 在训练身份认证模板时, 不是针对用户在某一类场景或某一类(几类)应用程序中的行为建立身份认证模板, 而是对用户的单次触屏行为建立身份认证模板。

2) 已有的方案无法保证会话内操作稀疏时的身份认证效果, 主要原因是这些身份认证机制以会话为单位提取用户行为特征(比如: 设置固定时间段作为一个会话, 获取该时间段内的用户行为特征, 或要求用户完成一组指定的任务作为一个会话)。由于无法保证攻击者的行为满足如上会话

要求, 所以难以保证身份认证效果。

为避免 TouchAuth 中存在如上缺陷, 本文的身份认证机制具备如下特点:

- 未采用会话作为提取用户行为特征的单位, 而是以单次触屏行为为单位提取用户行为特征;
- 判断单次触屏行为的合法性, 当非法触屏行为次数超过一定阈值后认定为非法用户。

攻击者如果需要查看用户移动终端上的内容通常需要进行触屏操作。TouchAuth 通过非法触屏行为的次数判断用户身份的合法性, 因此只要攻击者的触屏行为操作超过一定次数则可被 TouchAuth 识别。

4.2.2 触屏行为特征选择依据

不同的用户手掌大小不同, 力度及触屏习惯等不同导致其单次触屏行为的规律性也不同。TouchAuth 的输入为单次触屏行为的特征, 无论用户的触屏位置、触屏操作类型如何变化, 其单次触屏行为(比如: 用户的一次触屏行为在屏幕某一位置上的压力大小、停留时间等)会保持一定规律。

为表征如上规律, 本文从公开数据集 UMDAA- 02[26]中随机选取了两个用户, 分别命名为 User1 和 User2。User1 和 User2 的触屏行为数据(包括 UMDAA-02[26]中的训练数据和测试数据)分别被分为 5 等份。图 2、图 3 统计了每份数据的如下特征: 不同屏幕位置被触屏行为覆盖的比例(图 2、图 3 中每个格子里的数字为此区域被触屏行为覆盖的百分比)。从图 2、图 3 中可以看出: 相同用户的 5 份数据中, 相似的屏幕位置被触屏行为覆盖比例大体一致。不同用户, 相似屏幕位置被触屏行为覆盖比例有较大差异。

为表征用户触屏行为在屏幕某一区域内压力、停留时间、触屏动作类型的规律性, 我们完成了如下工作: 第一步, 选取 User1 和 User2 的触屏行为覆盖概率都较高的屏幕区域: 横坐标 $X \in (1119:1439)$, 纵坐标 $Y \in (674:809)$; 第二步, 分别提取出 User1 和 User2 所有满足 $X_{i(g)} \in (1199:1439)$ 且 $Y_{i(g)} \in (674:809)$ 的触屏行为数据 S_i^g; 第三步, 将提取出的数据分为 5 等份。User1 的 5 等份数据被命名为: 0101、0102、0103、0104、0105; User2 的 5 等份数据被命名为: 0201、0202、0203、0204、0205; 第四步, 分别统计 User1 和 User2 的 5 份数据中的触屏行为覆盖如下区间的百分比: 不同的触屏压力区间、不同的触屏停留时间区间、不同的触屏动作类型(如图 4~图 6 所示)。

图 4 中的横坐标代表压力区间, 纵坐标代表此压力区间被触屏行为覆盖的百分比。

图 5 中横坐标代表触屏停留时间区间(本文使用数据集 UMDAA-02[26]中的两个采样点 N_i^{n+1} 与 N_i^n 的时间戳之差代表 N_i^n 的触屏停留时间), 纵坐标代表每个触屏停留时间区间被触屏行为覆盖的百分比。

图 6 的横坐标代表触屏动作类型(在数据集合 UMDAA-02[26]中的触屏动作类型共分为两种: 532 代表按下、533 代表抬起或滑动)。纵坐标代表这个触屏动作类型被触屏行为覆盖的百分比。

图 4~图 6 中每个区间内被用户触屏行为覆盖的多数统计结果在红色横线附近。

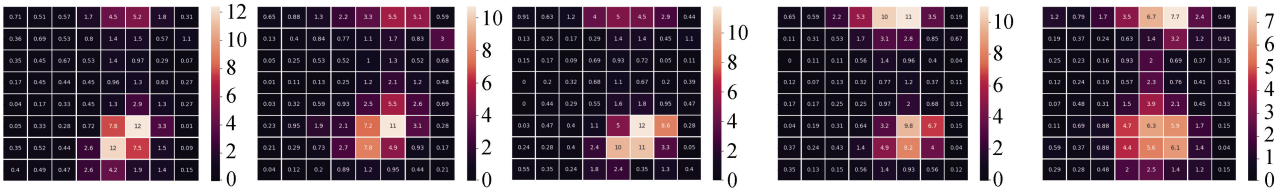

图 2 User1 触屏位置统计结果

Figure 2 Touch screen position statistics of Use1

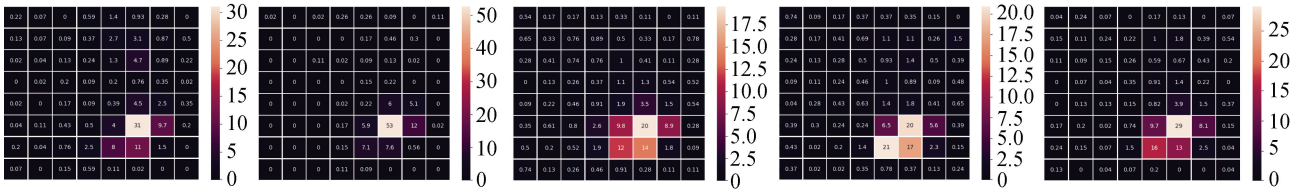

图 3 User2 触屏位置统计结果

Figure 3 Touch screen position statistics of User2

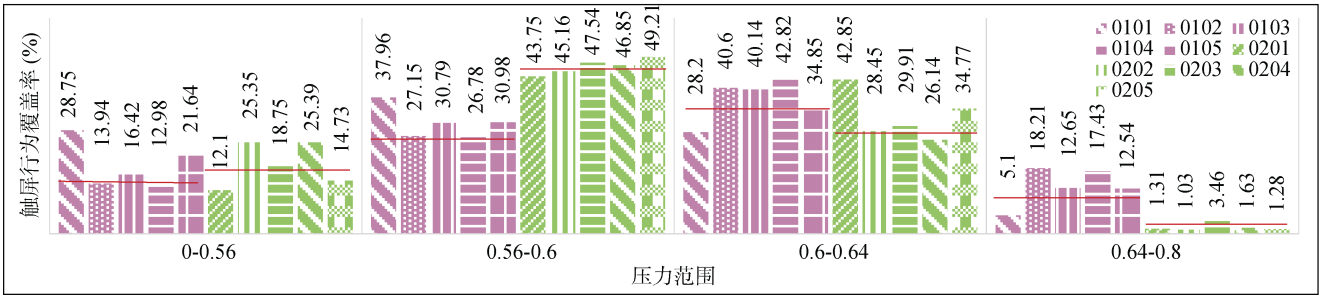

图 4　User1 和 User2 在屏幕横坐标 $X \in (1199:1439)$ 纵坐标 $Y \in (674:809)$ 区域的触屏压力统计

Figure 4　Touch screen press statistics of User1 and User2 in $X \in (1199:1439)$, $Y \in (674:809)$ of the screen

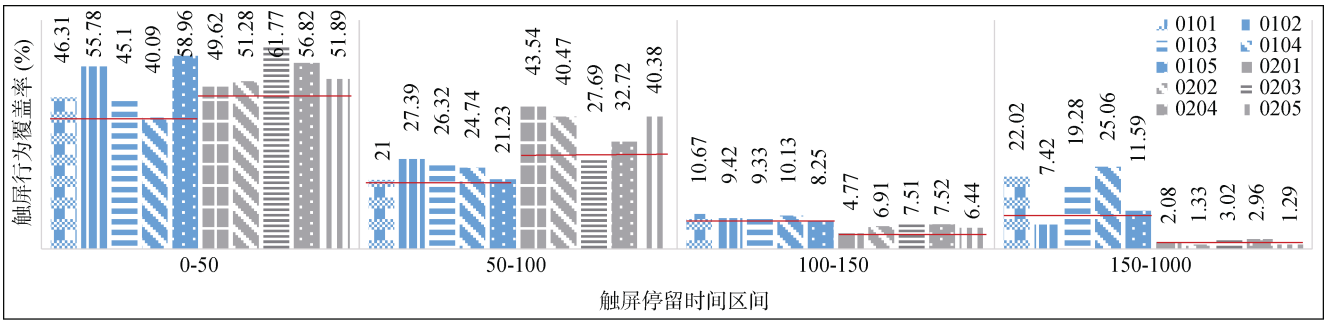

图 5　User1 和 User2 在屏幕横坐标 $X \in (1199:1439)$ 纵坐标 $Y \in (674:809)$ 区域的触屏停留时间统计

Figure 5　Touch screen time statistics of User1 and User2 in $X \in (1199:1439)$, $Y \in (674:809)$ of the screen

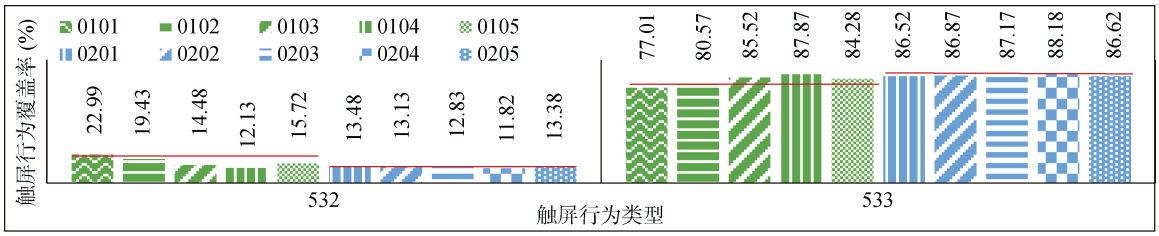

图 6　User1 和 User2 在屏幕横坐标 $X \in (1199:1439)$ 纵坐标 $Y \in (674:809)$ 区域的触屏动作类型统计

Figure 6　Statistics of touch screen action types of User1 and User2 in $X \in (1199:1439)$, $Y \in (674:809)$ of the screen

从图 4~图 6 中可以看出: 同一用户的同一触屏停留时间/压力区间(或触屏动作类型)被触屏行为覆盖比例在多数情况下大体一致。不同用户, 同一触屏停留时间/压力区间(或触屏动作类型)被触屏行为覆盖比例有较大差异。

基于如上分析本文判断身份的输入是用户的单次触屏行为数据, 该触屏行为数据会涉及触屏位置、触屏压力、停留时间、动作类型。为保证身份识别算法能够对一次触屏行为的触屏位置、触屏压力、停留时间等规律性进行关联分析。我们将单次触屏行为被采样后的数据作为身份判别模板的输入, 采样方式如下所述。

4.3　行为特征采样

本文提出一种支持多属性关联的行为特征采样方法, 如下将介绍行为特征采样方法及其依据。

定义 1: N_i 被采样后的数据为 $S_i = \{S_i^{(0)},\ldots,S_i^{(m-1)}\}$, 其中采样值 m 为一次触屏行为 N_i 数据被采样后的数据序列中的数据点的个数。

定义 2:

1) 如果触屏行为数据 $N_i = \{N_i^{(0)},N_i^{(1)},\ldots,N_i^{(n)}\}$ 的 $n < m-1$ 则 N_i 被丢弃。

如果采样值 m 过小, 比如 $m=2$ 时 N_i 被采样后的数据为 $S_i = \{S_i^{(0)},S_i^{(1)}\}$, 其中仅包含一次触屏行为被采集到的开始点和结束点的数据, 会丢失触屏行为的大量中间数据特征。而如果采样值过大会导致大量的触屏行为被丢弃。因此, 本文选择的采样

值 m 为 3、5, 并在试验部分对两种采样值的身份认证效果进行对比。

2) 具体采样方法为:

$$m=3\Rightarrow S_i=\left(N_i^0,N_i^{(n/2)^{\$}},N_i^n\right)$$

$$m=5\Rightarrow S_i=\left(N_i^0,N_i^{((n/2)^{\$}/2)^{\$}},N_i^{(n/2)^{\$}},N_i^{\left(((n/2)^{\$}+n)/2\right)^{\$}},N_i^n\right)$$

其中, $x^{\$}$ 代表的意思为: 如果 x 不是整数, 则 $x=x$ 的整数部分+1。

$$\left\{S_i^0,...,S_i^{\mathrm{g}},...,S_i^{m-1}\right\}=\left\{\begin{array}{c}\langle TT_{i(0)},X_{i(0)},Y_{i(0)},TY_{i(0)},P_{i(0)}\rangle\\ \bullet\\ \bullet\\ \langle TT_{i(g)},X_{i(g)},Y_{i(g)},TY_{i(g)},P_{i(g)}\rangle\\ \bullet\\ \bullet\\ \langle TT_{i(m-1)},X_{i(m-1)},Y_{i(m-1)},TY_{i(m-1)},P_{i(m-1)}\rangle\end{array}\right\}$$

作为行为分类器的输入数据, 可以支持行为分类器将每一次触屏行为的各个采样点 S_{i}^g 中的触屏位置 $\left(X_{i(g)},Y_{i(g)}\right)$、停留时间 $T_{i(g)}$、压力大小 $P_{i(g)}$、触屏动作类型 $TY_{i(g)}$ 的规律进行关联学习。

4.4 行为分类器

我们将每次触屏行为被采样后的数据 $\left\{S_i^0,...S_i^{\mathrm{g}},...,S_i^{m-1}\right\}$ 作为行为分类器的输入, 行为分类器通过学习其特征, 为每个用户构建触屏行为模板。并基于此行为模板判断用户触屏行为的合法性。

行为分类器的架构如图 7 所示。行为分类器共分为窗口层和认证层。窗口层将采样后的数据集合划分为固定大小的数据段, 并将各个数据段输入认证层。认证层对输入的数据段进行计算, 给出此次触屏行为是否为合法行为。

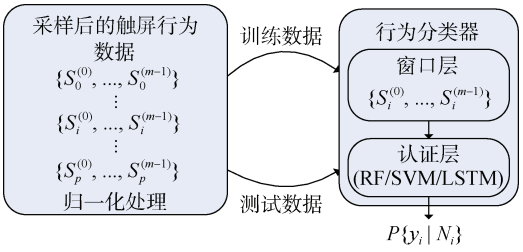

图 7 行为分类器架构

Figure 7 Architecture of behavior classifier

1) 窗口层

窗口大小等于采样值 m, 即每一个触屏行为 N_i 被采样后的长度。窗口层的输入数据被划分为各个数据段 $\left\{S_i^{(0)},...,S_i^{(m-1)}\right\}$, 得到特征数据段集 $F1-score=\dfrac{Recall*Precision}{Recall+Precision}$, 其中 p 为触屏行为 N_i 总个数。特征数据经过窗口层划分后即可输入到认证层。

2) 认证层

认证层学习用户行为特征, 能够根据用户历史行为数据判断本次数据段 $\left\{S_i^{(0)},...,S_i^{(m-1)}\right\}$ 代表的行为是否为合法行为。结果为二元分类中的一个的概率 $P\left\{\mathrm{y}_i\mid S_i:(S_i^{(0)},...,S_i^{(m-1)})\right\}$, 其中 $y_i=\{0,1\}$, 0 代表非法行为, 1 代表合法行为。

在认证层, 我们分别采用了 3 种算法进行身份认证。并将在实验部分对比 3 种算法的认证效果。这 3 种算法为: LSTM(Long Short-Term Memory)、RF(Random Forest)[40]、SVM(Support Vector Machines)。如下将对本层采用的每种算法的详细情况进行介绍。

• LSTM

本文采用 3 层单项 LSTM, 具体网络模型结构及参数如表 2 所述。

3 层单项 LSTM 的隐藏层分别由 256、120、60 个 LSTM 单元组成。输出层是一个 Sigmod 层, 输出单元表示此输入被认证为合法行为的概率。

我们选择均方误差(MSE, Mean Square Error)损失函数作为 LSTM 算法的损失函数。同时使用 Adam 算法[41]来优化模型的损失函数。

表 2 LSTM 网络模型结构及参数

Table 2 LSTM network model parameters

Layer(type)	Output Shape	Param #
dense_1(Dense)	(None,None,256)	6656
activation_1(Activation)	(None,None,256)	0
dropout1(Dropout)	(None,None,256)	0
dense_2(Dense)	(None,None,120)	30840
activation_2(Activation)	(None,None,120)	0
Dropout2(Dropout)	(None,None,120)	0
dense_3(Dense)	(None,None,60)	7260
activation_3(Activation)	(None,None,60)	0
dropout3(Dropout)	(None,None,60)	0
dense_4(Dense)	(None,None,1)	61
activation_4(Activation)	(None,None,1)	0

• RF

设置并行作业数量为–1, 作业数目为核心数。指定 RF 中的分类器的个数为 10。

• SVM

我们选择径向基函数(RBF, Radial Basis Function)作为核函数。

4.5 身份决策器

身份决策器综合计算一定决策步长内的非法行为个数, 得出此步长内的行为集合是否为合法用户的行为集合。当决策步长内的非法行为个数超过阈值时, 则此决策步长内的触屏行为集合被认定为非法用户的触屏行为集合。

决策步长为 k, 阈值为 t, 具体计算方法为:

对于触屏行为集 $(N_0,...,N_i,...,N_{k-1})$, 如果 $\sum_{i=0}^{k} P(N_i) < (k-t)$ 则此触屏行为集$(N_0,...,N_i,...,N_{k-1})$被认为是非法用户行为集。

决策步长大小决定了身份决策器需要依据多少次触屏行为来判断用户身份, 同时也在一定程度上决定了一次身份认证所需要的时间。决策步长越小, 认证相对越快, 但同时会减少用于推测用户身份的行为数量, 这会导致 TouchAuth 认证准确率降低, 而决策步长变大通常会使攻击者更容易窃取用户移动终端中的信息。

TouchAuth 是基于多次触屏行为的合法性判断用户身份。实际应用场景中, 当用户有新的触屏行为时, 将触屏行为数据输入 TouchAuth 可实时判定用户身份。因此 TouchAuth 可以避免用户未触屏查看移动终端时的无效身份鉴别, 同时确保用户在触屏查看移动终端信息时进行隐式、持续的身份认证。

5 实验

5.1 实验环境与评测指标

身份认证机制最常用的效果衡量指标为: 准确率(*Accuracy*)、错误接受率(*FAR*)、错误拒绝率(*FRR*)、等错误率(*EER*)和 *F*1-*score*。因此我们将准确率、*FAR*、*FRR*、*EER*、*F*1-*score* 作为 TouchAuth 的效果评价指标。

1) 准确率(*Accuracy*): 分类器正确分类的样本数与总样本数之比;

2) 错误接受率(*False Acceptance Rate, FAR*): 非法用户被归类为合法用户的可能性;

3) 错误拒绝率(*False Rejection Rate, FRR*): 合法用户被归类为非法用户的可能性;

4) 等误率(*Equal Error Rate, EER*): 通过调整阈值, 使得 *FRR* 等于 *FAR*, 此时的 *FAR* 与 *FRR* 的值称为等错误率;

5) *F*1-*score*: 精确率(*Precision*)和召回率(*Recall*)的调和平均数。

其中准确率(*Accuracy*)、*F*1-*score*、*FAR*、*FRR*、*EER* 的计算公式如下所述。

$$Accuray = \frac{TP + TN}{P + N} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$F1 - score = \frac{Recall * Precision}{Recall + Precision} \tag{4}$$

$$FAR = \frac{FP}{FP + TN} \tag{5}$$

$$FRR = \frac{FN}{FN + TP} \tag{6}$$

其中, 正例(*Positive,P*): 是指正例数据。

负例(*Negative,N*): 是指负例数据。

真阳性(*True Positive,TP*): 是指被分类器正确分类的正例数据。

真阴性(*True Negative,TN*): 是指被分类器正确分类的负例数据。

假阳性(*False Positive,FP*): 被标记为正例数据的负例数据。

假阴性(*False Negative,FN*): 被标记为负例数据的正例数据。

本实验将从如下几个方面对 TouchAuth 的效果进行评估:

1) 在特征采样值、决策步长及阈值取不同值的情况下, 采用第 4 章中所介绍的 3 种算法(RF、SVM、LSTM)计算 TouchAuth 的身份识别效果(*FAR*、*EER*、*FRR*、*F*1-*score*、准确率);

2) 适应性验证: 验证 TouchAuth 在特殊情况(比如用户新安装了一个应用程序的场景)下的身份认证效果;

3) 与其他身份认证方案进行对比, 包括: 与使用本实验同样数据集合 UMDAA-02[26]验证身份识别效果的其他方案的对比; 与已有的基于触屏行为的典型身份识别方案的对比。

5.2 数据集

本文的实验采用两类数据集合:

一类为公开数据集合 UMDAA-02[26] 。该数据集合为 45 个志愿者使用 Nexus5 两个月的时间内被采集的行为数据。由于其中一些志愿者的数据不齐全, 本实验选取了该数据集合中数据齐全的 30 个志愿者的数据作为本实验的数据集合。

另一类为本实验随机选择的 15 位志愿者按本

文实验步骤(如下文 5.4 节所述)要求使用移动终端, 移动终端中的触屏行为采集软件在此过程中采集志愿者的触屏行为数据。这些志愿者的年龄在 20 岁到 60 岁之间, 都具备两年以上的 Android 移动终端使用经验。

5.3 3 种算法的认证效果对比

本节采用公开数据集合 UMDAA-02[26] 评估 3 种算法的认证效果。

公开数据集合 UMDAA-02[26]中每个用户的触屏行为数据被分为测试集合和训练集合。在本实验中, 我们将每个用户的测试集合数据和训练集合数据进行合并作为该用户的正样本数据。

行为分类器使用来自合法用户和非法用户的数据训练用户行为模板。来自合法用户的数据被标记为正, 而来自非法用户的数据被标记为负。在训练模型时, 我们使用来自合法用户的所有正样本数据和非法用户(随机选择的 10 个其他用户)的数据作为负样本数据, 正负样本数据量相等。

我们使用分层十倍交叉验证方法对 TouchAuth 进行评估。最终得出的评估结果(*FAR*、*FER*、*FRR*、*F1-score*、准确率)是 10 个结果的平均值。

本节评估在不同的行为特征采样值 *m*、决策步长 *k* 及阈值 *t* 设置下, 3 种算法(RF、SVM、LSTM)的身份认证效果(*FAR*、*FRR*、*EER*、*F1-score*、准确率), 如图 8~图 12 所示。其中 *m, k, t* 的取值范围:

1) $m \in (3,5)$;

2) $(k,t) \in \{(10,4),(15,6),(20,7)\}$;

从图 8~图 12 可以得出如下结论:

1) 行为特征采样值 *m* 为 5 时的身份认证效果优于 *m* 为 3 时的身份认证效果;

2) 随着决策步长 *k* 和阈值 *t* 的值变小, 每种算法的各项评估结果都在下降;

3) 无论决策步长或阈值如何改变, 三种算法效果的优劣保持不变: RF 算法的效果最好; LSTM 算法效果略差于 RF 算法的效果; SVM 算法的效果排第 3 位, 且与 LSTM 算法效果相差较多。

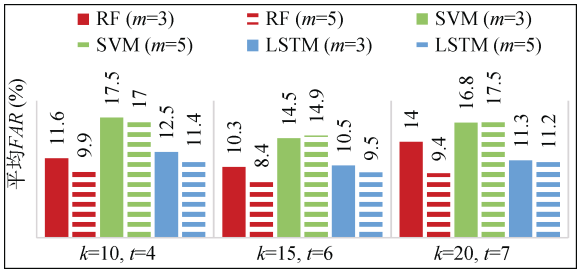

图 8 平均 *FAR*

Figure 8 Average *FAR*

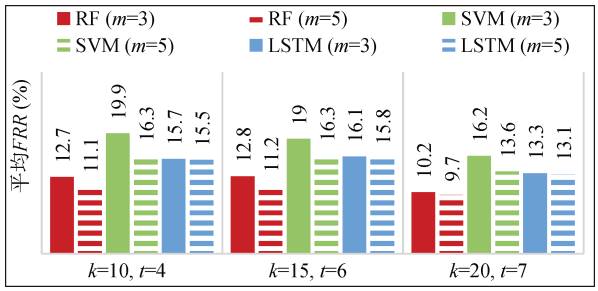

图 9 平均 *FRR*

Figure 9 Average *FRR*

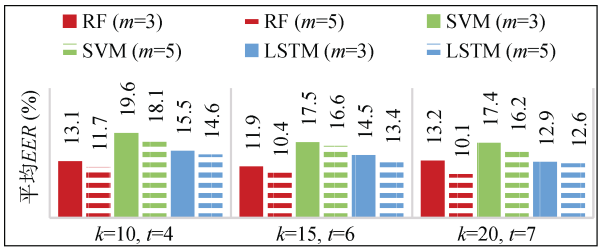

图 10 平均 *EER*

Figure 10 Average *EER*

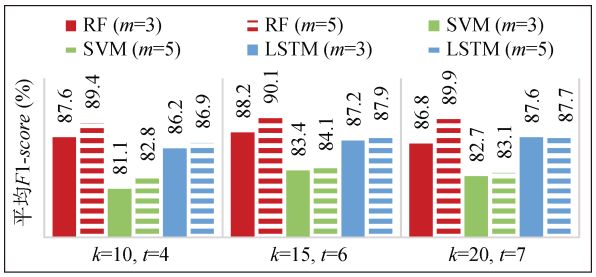

图 11 平均 *F1-score*

Figure 11 Average *F1-score*

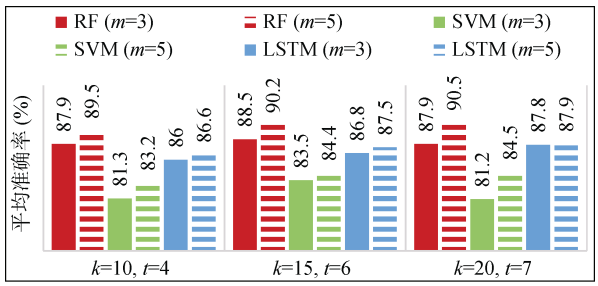

图 12 平均准确率

Figure 12 Average accurate

实验结果表明: 在采样值 *m* 为 5、决策步长 *k* 为 20、阈值 *t* 为 7 的情况下 RF 的算法效果最好, 平均 *FAR* 为 9.4%、平均 *FRR* 为 9.7%、平均 *EER* 为 10.1%、平均 F1-*score* 为 89.9%、平均准确率为 90.5%。

实验结果分析: 在此类应用场景下通常深度学习方法预期要比传统机器学习方法效果好, 但是由于 UMDAA-02[26]中的数据量较少, 未体现出深度学习方法的优势。

5.4 适应性验证

通常情况下当用户新安装一个应用程序后, 行为可能发生较大变化, 为验证 TouchAuth 在这些场景下的适应性, 本节进行如下实验:

1) 要求每位志愿者使用安装有触屏行为采集软件的移动终端 7 天的时间, 此时间段内志愿者可以依据自己的习惯随意使用移动终端上的任何应用程序, 其行为不受任何限制;

2) 志愿者使用移动终端 7 天后, 我们采用 5.3 节筛选出的身份认证效果较好的 RF 算法, 用采集到的触屏行为数据为每位志愿者建立身份认证行为模板。其中, 用于训练模板的负样本来自除该志愿者以外的自其他志愿者, 如果负样本数据量不够则从数据集合 UMDAA-02[26]中随机选取用户数据进行补充, 以保证正负样本数量一致;

3) 为每位志愿者建立身份认证行为模板后, 我们采用 5.3 节筛选出的身份认证效果较好的决策步长 k 为 20、阈值 t 为 7 的参数设置, 对使用移动终端的用户的身份进行实时判断;

4) 实时判断分为两种情况, 第一种情况是志愿者使用自己的移动终端 2 小时, 在这 2 小时中每一名志愿者需要随机从应用市场中至少下载一个新的应用程序安装并使用。第二种情况是志愿者使用其他志愿者的移动终端 2 小时, 在这 2 小时中使用者需要随机从应用市场中至少下载一个新的应用程序安装并使用。

实时判断实验结果为: 平均 *FAR* 为 10.8%、平均 *FRR* 为 10.2%、平均 *EER* 为 11.9%、平均 *F*1-*score* 为 87%、平均准确率为 89.6%。由如上结果可看出在用户新安装了一个(或几个)新应用程序的情况下 TouchAuth 的身份认证效果略有下降, 但是下降幅度较小。

5.5 不同方法对比

由 5.3 的实验结果得出 RF 整体效果优于其他算法, 因此本文采用 m=5、k=20、t=7 且行为分类器采用 RF 算法时 TouchAuth 的身份效果(其身份识别效果为 5.3 节与 5.4 节实验结果的平均值: *FAR* 为 10.1%、*FRR* 为 9.95%、*EER* 为 11%、*F*1-*score* 为 88.45%、准确率 90.05%)与其他方案进行对比。本节主要从如下两个方面进行对比:

5.5.1 与使用 UMDAA-02[26]数据集合验证身份认证效果的方案对比

使用 UMDAA-02[26]数据集合进行身份认证的方案主要有两个: 方案[27]对此数据集合中的触屏行为数据提取 21 种触屏行为特征, 并使用 6 种算法进行身份识别, 其中效果最好的算法为 RF, *EER* 为 22%。方案[28]使用了此数据集合中的应用程序使用情况的相关数据进行身份认证, 未使用此数据集合中的触屏行为数据, 其 *EER* 为 31.93%。

本节从如下两个方面进行对比(对比结果如表 3 所示): 1) 实验效果; 2) 检测到攻击者的延迟。

表 3 与其他方案对比 1

Table 3 Comparison of TouchAuth and other schemes1

	方案[27]	方案[28]	TouchAuth
ERR	22%	31.93%	11%
延迟	文中未提及	2.5 分钟	攻击者进行 7 次本文定义的触屏行为

实验结果分析:

1) 与这两种方案相比, TouchAuth 的 *EER* 分别比这两种方案减少了 11%和 20.93%;

2) 方案[27]未介绍检测到攻击者的延迟。方案[28]可在 2.5 分钟内检测到攻击者; 攻击者仅完成 7 次本文定义的触屏行为就可以被 TouchAuth 检测到。

5.5.2 与使用触屏行为数据进行隐式持续身份认证的方案对比

本实验选取了 5 种典型的仅使用触屏行为数据的隐式、持续身份认证方案。从如下几个方面将 TouchAuth 与这些方案进行对比(对比结果如表 4 所示):

1) 身份认证效果是否局限于某一类场景或某一类(几类)应用程序;

2) 是否可以在会话期间操作稀疏的情况下保证身份认证效果;

3) 实验所用数据集合是包含不可控数据;

4) 身份认证效果(参与对比的 5 个方案中并不是每个方案都描述了平均 *EER*、平均 *F*1-*score*、准确率, 本文根据这些方案中给出的实验效果指标与 TouchAuth 相应的实验效果指标进行对比)。

表 11 中可以看出 1), 2), 3)三个方面全部为‘是’的只有 TouchAuth。本文从如下几个方面分析表 11 的对比结果:

1) 与仅具备如下特征的方案的对比结果进行分析: 身份认证效果局限于某一类场景或某一类(几类)应用程序;

TouchAuth 在身份认证过程中仅使用用户的触屏行为数据, 认证过程未涉及应用程序与或应用场景相关的因素。使用的实验数据为 30 个用户两个月日常使用移动终端的触屏行为数据, 此过程中用户所使用的应用程序、使用场景等完全由用户随机决定。与局限于某一类场景或某一类(几类)应用程序的文献[25]对比, 二者的准确率几乎一致。

表 4　与其他方案对比 2

Table 4　Comparison of TouchAuth and other schemes2

	文献[23]	文献[25]	文献[22]	文献[24]	文献[32]	TouchAuth
1) 是否局限于某一类或几类应用程序	是	是	是	是	否	是
2) 是否可以在会话期间操作稀疏的情况下保证身份认证效果	否	是	否	否	否	是
3) 数据集合是否不可控	否	否	否	否	否	是
4) 身份认证效果	*EER* 为 11.5%	准确率为 90%	平均 *EER* 为 7%, 平均准确率为 93%	平均 *EER* 为 2.4%	平均 *EER* 为 7.8%	平均 *EER* 为 11%、平均 *F*1-*score* 为 88.45%、平均准确率为 90.05%

2) 与仅具备如下特征的方案的对比结果进行分析: 无法保证会话期间操作稀疏时的身份认证效果;

TouchAuth 在身份认证过程中根据多次触屏行为的合法性判断用户身份, 不是以会话为单位判断用户身份, 身份认证效果不受会话影响。文献[32]的平均 *EER* 比 TouchAuth 低 3.2%, 但是此方案在身份认证中对用户操作的要求较高, 其实验需要用户每操作移动终端 10 分钟作为一个会话, 如果不符合要求需要用户重新生成会话。用户实际使用中很可能难以达到实验中所要求的条件, 认证效果可能受到影响。

3) 与具备如下特征的方案的对比结果进行分析: 身份认证效果局限于某一类场景或某一类(几类)应用程序, 而且无法保证会话期间操作稀疏时的身份认证效果;

文献[23]的 *EER* 高于 TouchAuth 的平均 *EER*、文献[22]的平均准确率和平均 *EER* 略高于 TouchAuth 的相应指标。文献[24]的 *EER* 比 TouchAuth 低 8.6%, 但是此方案的身份认证效果仅局限于浏览器类应用程序, 且认证过程对用户要求较多(类似于方案文献[32]具有的缺点), 因此其保护用户隐私数据不被非法查看的效果较为有限。

通过如上比较结果可得出: TouchAuth 身份认证效果不局限于某一场景或某一类(几类)应用程序, 且不存在会话期间操作稀疏可能导致的身份认证效果差的问题。

6　结论及未来工作

为解决传统的身份验证方法在用户通过初始身份验证后不能提供持续的保护从而导致隐私泄露的问题, 本文提出了一种支持多属性关联的特征采样方法及基于用户触屏行为驱动的隐式持续身份认证机制—TouchAuth。TouchAuth 基于对用户触屏行为的采样数据, 综合多个触屏行为的合法性判断用户身份。TouchAuth 仅基于用户触屏行为认证用户身份, 不涉及过多用户隐私信息; 仅在用户查看手机内容时进行持续隐式身份认证, 有效避免了用户未查看移动终端时的无效身份认证。在公开数据集合上的大量实验结果证明 TouchAuth 的身份认证效果不受场景或应用程序限制、克服了会话内操作稀疏时身份认证效果无法保证的问题。攻击者仅完成 7 次本文定义的触屏行为就可以被 TouchAuth 检测到, 平均 *EER* 为 11%。

在实际使用场景中, 身份认证机制需要在 *FAR*(安全性)和 *FRR*(可用性)之间进行权衡。从安全性的角度来看, 错误拒绝比错误接受代价低, 因为较高的错误接受率会大大降低身份认证的安全性。相比之下, 更高的错误拒绝率会降低可用性, 在现实场景中, 一个合适的用户身份认证系统需要同时实现较低的 *FAR* 和较低的 *FRR*。

为了提高安全性, 本文所提方法牺牲了一定的可用性, 因此未来需要继续优化身份识别算法以达到更低的 *FAR* 和 *FRR*。比如: 可以将深度学习算法中的 LSTM 及 CNN 相结合从时间和空间两个维度构建更为精准的身份认证模型。此外, 深度学习通常需要海量样本才能有效学习用户触屏行为的本质特征。本实验的实验数据需要人为采集, 如果要达到海量样本需要志愿者长时间使用采集触屏行为的移动终端, 此特性会导致数据采集难度较大。由于数据采集难度较大, 当前学术界所能提供的可用的包含用户触屏行为特征的公开数据集合很少[28], 当前适合本实验的公开数据集合仅有 UMDAA-02[26]。文献[28]针对数据集合 UMDAA-02[26]中的应用程序使用记录实现对用户身份的识别, 该文献指出可以使用 RNN 来学习更多的用户使用应用程序的行为模式, 但是由于 RNN 需要大量数据, 已有公开数据集合数据量难以满足此需求。因此如何自动化构建高质量的海量用户触屏行为数据集将是未来工作的重要方向。

参考文献

[1] https://www.idc.com/promo/smartphone-market-share/os.

[2] Kim, Youngho, Tae Oh, and Jeongnyeo Kim. Analyzing user awareness of privacy data leak in mobile applications[J]. M*obile Information Systems*, 2015(pt.2): 1-12.

[3] Kim Y, Oh T, Kim J. Analyzing User Awareness of Privacy Data Leak in Mobile Applications[J]. *Mobile Information Systems*, 2015, 2015: 1-12.

[4] Sarsavadia, Riddhi, and Usha Patel. A Survey on Intelligent Face Recognition System[C]. *International Conference on ISMAC in Computational Vision and Bio-Engineering*, 2018: 1209-1215.

[5] Sarsavadia R, Patel U. A Survey on Intelligent Face Recognition System[C]. *International Conference on ISMAC in Computational Vision and Bio-Engineering*, 2019: 1209-1215.

[6] Ali, Mouad MH, and A. T. Gaikwad. Multimodal biometrics enhancement recognition system based on fusion of fingerprint and palmprint: a review[J]. *Global Journal of Computer Science and Technology*, 2016.

[7] Ali M M H, Mahale V H, Yannawar P, et al. Overview of fingerprint recognition system[C]. *2016 International Conference on Electrical, Electronics, and Optimization Techniques*, 2016: 1334-1338.

[8] Ali M M H, Mahale V H, Yannawar P, et al. Overview of Fingerprint Recognition System[C]. *2016 International Conference on Electrical*, *Electronics*, *and Optimization Techniques*, 2016: 1334-1338.

[9] Umer, Saiyed, Bibhas Chandra Dhara, and Bhabatosh Chanda. A novel cancelable iris recognition system based on feature learning techniques[J]. *Information Sciences*, 2017, 406: 102-118.

[10] Umer S, Dhara B C, Chanda B. A Novel Cancelable Iris Recognition System Based on Feature Learning Techniques[J]. *Information Sciences*, 2017, 406/407: 102-118.

[11] Neal T J, Woodard D L. Surveying biometric authentication for mobile device security[J]. *Journal of Pattern Recognition Research*, 2016, 1.74-110: 4.

[12] Neal T, Woodard D. Surveying Biometric Authentication for Mobile Device Security[J]. *Journal of Pattern Recognition Research*, 2016, 11(1): 74-110.

[13] Crawford, Heather, Renaud, Karen. Understanding user perceptions of transparent authentication on a mobile device[J]. *Journal of Trust Management*, 2014, 1.1: 7.

[14] Crawford H, Renaud K. Understanding User Perceptions of Transparent Authentication on a Mobile Device[J]. *Journal of Trust Management*, 2014, 1(1): 1-28.

[15] Khan, Hassan, Urs Hengartner, and Daniel Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying[C]. *Eleventh Symposium On Usable Privacy and Security,* 2015: 225-239.

[16] Patel, Vishal M, et al. Continuous user authentication on mobile devices: Recent progress and remaining challenges[J]. *IEEE Signal Processing Magazine*, 2016, 33.4: 49-61.

[17] 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.

[18] Kambourakis G, Damopoulos D, Papamartzivanos D, et al. Introducing touchstroke: keystroke‐based authentication system for smartphones[J]. *Security and Communication Networks*, 2016, 9.6: 542-554.

[19] Kambourakis G, Damopoulos D, Papamartzivanos D, et al. Introducing Touchstroke: Keystroke-Based Authentication System for Smartphones[J]. *Security and Communication Networks*, 2016, 9(6): 542-554.

[20] Mondal S, Bours P. Person identification by keystroke dynamics using pairwise user coupling[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12.6: 1319-1329.

[21] Mondal S, Bours P. Person Identification by Keystroke Dynamics Using Pairwise User Coupling[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(6): 1319-1329.

[22] Buriro A, Crispo B, Gupta S, et al. Dialerauth: A motion-assisted touch-based smartphone user authentication scheme[C]. *Proceedings of The Eighth ACM Conference on Data and Application Security and Privacy*, 2018: 267-276.

[23] Buriro A, Crispo B, Gupta S, et al. DIALERAUTH: A Motion-Assisted Touch-Based Smartphone User Authentication Scheme[C]. *The Eighth ACM Conference on Data and Application Security and Privacy*, 2018: 267-276.

[24] WH Lee, X Liu, Y Shen, et al. Secure pick up: Implicit authentication when you start using the smartphone[C]. *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, 2017: 67-78.

[25] Lee W H, Liu X C, Shen Y L, et al. Secure Pick Up: Implicit Authentication when You Start Using the Smartphone[C]. *The 22nd ACM on Symposium on Access Control Models and Technologies*, 2017: 67-78.

[26] Zhu T, Qu Z, Xu H, et al. RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild[J]. *IEEE Transactions on Mobile Computing*, 2019, 19.2: 466-483.

[27] Zhu T T, Qu Z Y, Xu H T, et al. RiskCog: Unobtrusive Real-Time User Authentication on Mobile Devices in the Wild[J]. *IEEE Transactions on Mobile Computing*, 2020, 19(2): 466-483.

[28] 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*, 2016, 11.2: 513-521.

[29] 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.

[30] Jonathan Voris, Yingbo Song, Malek Ben Salem, et al. You Are What You Use: An Initial Study of Authenticating Mobile Users via Application Usage[C]. *Proceedings of the 8th EAI International Conference on Mobile Computing, Applications and Services*, 2016: 51-61.

[31] Voris J, Song Y B, Ben Salem M, et al. You are what You Use: An Initial Study of Authenticating Mobile Users via Application Usage[C]. *The The 8th EAI International Conference on Mobile Computing*, *Applications and Services*, 2016: 51-61.

[32] Zou Q, Wang Y, Wang Q, et al. Deep Learning-Based Gait Recognition Using Smartphones in the Wild[C]. *IEEE Transactions on Information Forensics and Security,* 2020, 15: 3197-3212.

[33] Zou Q, Wang Y L, Wang Q, et al. Deep Learning-Based Gait Recognition Using Smartphones in the Wild[C]. *IEEE Transactions on Information Forensics and Security*, 2020: 3197-3212.

[34] Abuhamad M, Abuhmed T, Mohaisen D, et al. AUToSen: Deep Learning-based Implicit Continuous Authentication Using Smartphone Sensors[J]. *IEEE Internet of Things Journal*, 2020, 7(6): 5008-5020.

[35] Abuhamad M, Abuhmed T, Mohaisen D, et al. AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors[J]. *IEEE Internet of Things Journal*, 2020, 7(6): 5008-5020.

[36] https://www.comscore.com/Insights/Blog/Mobile-Matures-as-the-Cross-Platform-Era-Emerges.

[37] van Berkel N, Luo C, Anagnostopoulos T, et al. A systematic assessment of smartphone usage gaps[C]. *The 2016 CHI Conference on Human Factors in Computing Systems*, 2016: 4711-4721.

[38] van Berkel N, Luo C, Anagnostopoulos T, et al. A Systematic Assessment of Smartphone Usage Gaps[C]. *The 2016 CHI Conference on Human Factors in Computing Systems*, 2016: 4711-4721.

[39] Sharma V, Enbody R. User authentication and identification from user interface interactions on touch-enabled devices[C]. *The 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017: 1-11.

[40] Sharma V, Enbody R. User Authentication and Identification from User Interface Interactions on Touch-Enabled Devices[C]. *The 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017: 1-11.

[41] Temper M, Tjoa S, Kaiser M. Touch to authenticate—Continuous biometric authentication on mobile devices[C]. *2015 1st International Conference on Software Security and Assurance*, 2015: 30-35.

[42] Temper M, Tjoa S, Kaiser M. Touch to Authenticate—Continuous Biometric Authentication on Mobile Devices[C]. *2015 1st International Conference on Software Security and Assurance*, 2017: 30-35.

[43] Meng W, Wang Y, Wong D S, et al. TouchWB: Touch behavioral user authentication based on web browsing on smartphones[J]. *Journal of Network and Computer Applications,* 2018, 117: 1-9.

[44] Meng W Z, Wang Y, Wong D S, et al. *TouchWB*: Touch Behavioral User Authentication Based on Web Browsing on Smartphones[J]. *Journal of Network and Computer Applications*, 2018, 117: 1-9.

[45] Feng T, Yang J, Yan Z, et al. Tips: Context-aware implicit user identification using touch screen in uncontrolled environments[C]. *The 15th Workshop on Mobile Computing Systems and Applications*, 2014: 1-6.

[46] Feng T, Yang J, Yan Z X, et al. TIPS: Context-Aware Implicit User Identification Using Touch Screen in Uncontrolled Environments[C]. *The 15th Workshop on Mobile Computing Systems and Applications*, 2014: 1-6.

[47] https://umdaa02.github.io/.

[48] Mahbub U, Sarkar S, Patel V M, et al. Active user authentication for smartphones: A challenge data set and benchmark results[C]. *2016 IEEE 8th international conference on biometrics theory, applications and systems*, 2016: 1-8.

[49] Mahbub U, Sarkar S, Patel V M, et al. Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results[C]. *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems*, 2016: 1-8.

[50] 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.

[51] 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.

[52] Sae-Bae N, Ahmed K, Isbister K, et al. Biometric-rich gestures: a novel approach to authentication on multi-touch devices[C]. *The SIGCHI Conference on Human Factors in Computing Systems*, 2012: 977-986.

[53] Sae-Bae N, Ahmed K, Isbister K, et al. Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-Touch Devices[C]. *The SIGCHI Conference on Human Factors in Computing Systems*, 2012: 977-986.

[54] De Luca A, Hang A, Brudy F, et al. Touch me once and I know it's you! implicit authentication based on touch screen patterns[C]. *The SIGCHI Conference on Human Factors in Computing Systems*, 2012: 987-996.

[55] De Luca A, Hang A, Brudy F, et al. Touch me once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns[C]. *The SIGCHI Conference on Human Factors in Computing Systems*, 2012: 987-996.

[56] 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.

[57] 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*, 2013, 8(1): 136-148.

[58] Meng Y, Wong D S, Schlegel R. Touch gestures based biometric authentication scheme for touchscreen mobile phones[C]. *International conference on information security and cryptology*, 2012: 331-350.

[59] Meng Y X, Wong D S, Schlegel R, et al. Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones[C]. *International Conference on Information Security and Cryptology*, 2013: 331-350.

[60] Zaliva V, Melicher W, Saha S, et al. Passive user identification using sequential analysis of proximity information in touchscreen usage patterns[C]. *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking*, 2015: 161-166.

[61] Zaliva V, Melicher W, Saha S Y, et al. Passive User Identification Using Sequential Analysis of Proximity Information in Touchscreen Usage Patterns[C]. *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking*, 2015: 161-166.

[62] Shahzad M, Liu A X, Samuel A. Behavior based human authentication on touch screen devices using gestures and signatures[J]. *IEEE Transactions on Mobile Computing*, 2016, 16(10): 2726-2741.

[63] Shahzad M, Liu A X, Samuel A. Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures[J]. *IEEE Transactions on Mobile Computing*, 2017, 16(10): 2726-2741.

[64] Van Nguyen T, Sae-Bae N, Memon N. DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices[J]. *computers & security*, 2017, 66: 115-128.

[65] Van Nguyen T, Sae-Bae N, Memon N. DRAW-a-PIN: Authentication Using Finger-Drawn PIN on Touch Devices[J]. *Computers & Security*, 2017, 66: 115-128.

[66] Ferreira D, Kostakos V, Beresford A R, et al. Securacy: an empirical investigation of Android applications' network usage, privacy and security[C]. *The 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 2015: 1-11.

[67] Ferreira D, Kostakos V, Beresford A R, et al. Securacy: An Em-

pirical Investigation of Android Applications' Network Usage, Privacy and Security[C]. *The 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015: 1-11.

[68] Shepard C, Rahmati A, Tossell C, et al. LiveLab: measuring wireless networks and smartphone users in the field[J]. *ACM SIGMETRICS Performance Evaluation Review*, 2011, 38(3): 15-20.

[69] Shepard C, Rahmati A, Tossell C, et al. LiveLab[J]. *ACM SIGMETRICS Performance Evaluation Review*, 2011, 38(3): 15-20.

[70] 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.

[71] Abuhamad M, Abusnaina A, Nyang D, et al. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey[J]. *IEEE Internet of Things Journal*, 2021, 8(1): 65-84.

[72] 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.

[73] Shen C, Li Y X, Chen Y F, et al. Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(1): 48-62.

[74] Breiman L. Random forests[J]. *Machine learning*, 2001, 45(1): 5-32.

[75] Breiman L. Random Forests[J]. *Machine Learning*, 2001, 45(1): 5-32.

[76] Kingma D, Ba J. Adam: A Method for Stochastic Optimization[J]. *Computer Science,* 2014.

[77] Kingma D P, Ba J. Adam: A Method for Stochastic Optimization[EB/OL]. 2014: arXiv: 1412.6980. https://arxiv.org/ abs/1412.6980.

马璐萍 于2021年在中国科学院大学网络空间安全专业获得博士学位，现任中国科学院信息工程研究所工程师。研究领域为移动互联网安全。研究兴趣包括操作系统安全、网络攻防。Email: maluping@iie.ac.cn

张顺亮 于2004年在浙江大学计算机科学与技术专业获得博士学位。现任中国科学院信息工程研究所高级工程师。研究领域为移动通信与安全、网络系统结构与安全防护。研究兴趣包括：5G/6G移动通信安全、智能网络安全防护，Email:zhangshunliang@iie.ac.cn

冯维淼 于2008年在北京大学计算机应用技术专业获得硕士学位，现在中国科学院信息工程研究所任高级工程师。研究领域为移动终端安全、无线局域网安全。研究兴趣包括：移动应用安全分析、终端安全管控、无线局域网攻防技术等。Email:fengweimiao@iie.ac.cn

张珠君 于2012年在北京交通大学通信与信息系统专业获得硕士学位。现在中国科学院大学网络空间安全专业攻读博士学位。现任中国科学院信息工程研究所工程师。研究领域为物联网安全。研究兴趣包括：物联网安全，区块链技术。Email: zhangzhujun@iie.ac.cn

朱大立 于2007年12月在华中科技大学计算机应用技术专业获得博士学位。现任中国科学院信息工程研究所第四研究室正研级高级工程师。研究领域为移动互联网安全。研究兴趣包括智能终端安全，无线网络空口协议安全。Email: zhudali@iie.ac.cn

马宇晨 于2015年在天津大学信息管理与信息系统专业得学士学位。现在中国科学院信息工程研究所第四研究室攻读博士学位。研究领域为网络表示学习、异常检测等。Email: mayuchen@iie.ac.cn

彭淑敏 于2005年在西安电子科技大学通信与信息系统专业获得硕士学位。现任郑州大学讲师。研究领域为无线通信。研究兴趣包括通信中的编解码、网络安全。Email:pengshumin@zzu. edu.cn