软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(8):2392−2414 [doi: 10.13328/j.cnki.jos.005760]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 Laplace 机制的普适运动传感器侧信道防御方案*

唐奔宵, 王丽娜, 汪 润, 赵 磊, 陈青松

(武汉大学 国家网络安全学院,湖北 武汉 430072)

通讯作者: 王丽娜, E-mail: lnwang@whu.edu.cn

摘 要: 针对移动设备中运动传感器侧信道的防御研究面临很多困难,已有的解决方案无法有效实现用户体验与防御能力之间的平衡,也难以覆盖各种类型的运动传感器侧信道.为了解决上述问题,系统地分析了运动传感器侧信道攻击的通用模型,针对侧信道构建过程,提出了一种基于差分隐私 Laplace 机制的传感器信号混淆方案.该方案实施于系统框架层,通过无差别地向传感器信号中实时注入少量受控噪声,干扰侧信道学习"用户行为-设备状态-传感器读数"之间的映射关系.构建了侧信道的通用模型,结合典型的侧信道,从理论层面详细地分析了信号混淆抵抗传感器侧信道攻击的原理,证明防御方案具有优异的普适性、可用性和灵活性,能够有效地对抗实验以外的已知或未知运动传感器侧信道攻击.最后,筛选出 11 种典型的运动传感器侧信道进行对抗实验,验证了该防御方案对抗实际攻击的有效性.

关键词: Andorid;运动传感器;侧信道攻击;隐私保护;差分隐私

中图法分类号: TP309

中文引用格式: 唐奔宵,王丽娜,汪润,赵磊,陈青松.基于 Laplace 机制的普适运动传感器侧信道防御方案.软件学报,2019,30(8):2392−2414. http://www.jos.org.cn/1000-9825/5760.htm

英文引用格式: Tang BX, Wang LN, Wang R, Zhao L, Chen QS. General side channel defense schema of motion sensor based on Laplace mechanism. Ruan Jian Xue Bao/Journal of Software, 2019,30(8):2392−2414 (in Chinese). http://www.jos.org.cn/1000-9825/5760.htm

General Side Channel Defense Schema of Motion Sensor Based on Laplace Mechanism

TANG Ben-Xiao, WANG Li-Na, WANG Run, ZHAO Lei, CHEN Qing-Song

(School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China)

Abstract: The privacy issue under the motion sensor-based side channel is a fundamental and critical research topic with many challenges. The existing solutions do not solve some significant problems in practice, for example, the protection mechanism should balance user experience with defensive effectiveness. Moreover, extra settings should not be required. As an effort towards this issue, the common pattern of motion sensor-based side-channel attacks is analyzed, and it finds that the key step of these side-channel attacks is learning the mapping relationship among user behavior, device status, and sensor reading. In addition, a protection method is proposed which applies differential privacy scheme and injects random noise to sensor readings indiscriminately to reduce the effect of learning mapping relationship. This defense method is implemented in system framework, thus it is transparent to both users and attackers. Moreover, the mechanism of proposed defense method is analyzed theoretically to demonstrate how this method decrease the attack

* 基金项目: 国家自然科学基金(61876134, 61672394); 国家重点研发计划(2016YFB0801100); 国家自然科学联合基金(U1536204)

Foundation item: National Natural Science Foundation of China (61876134, 61672394); National Key Research and Development Program of China (2016YFB0801100); Programs of Joint Funds of National Natural Science Foundation of China (U1536204)

本文由"面向自主安全可控的可信计算"专题特约编辑贾春福教授推荐.

收稿时间: 2018-05-21; 修改时间: 2018-09-21; 采用时间: 2018-12-13; jos 在线出版时间: 2019-03-28

CNKI 网络优先出版: 2019-03-29 09:16:40, http://kns.cnki.net/kcms/detail/11.2560.TP.20190329.0915.011.html

success rate and prove that this method can work for any other known and unknown motion sensor side-channel attacks. Finally, the proposed schema is evaluated by conducting experiments against 11 typical motion sensor-based side-channel attacks.

Key words: Android; motion sensor; side-channel attack; privacy protection; differential privacy

移动互联网、智能终端、位置服务等新技术的融合催生了移动应用和服务(简称 APP)的空前发展.借助于智能终端中的多样化传感器,面向个性化定制的移动应用更是为用户带来了丰富且便捷的生活体验.这其中,以加速度传感器、陀螺仪、方向传感器等为代表的运动传感器在 APP 中得到广泛应用.然而,移动服务的个性化定制依赖于个性化的数据采集,单个传感器或者多个传感器的组合可被攻击者用来区分用户的个体差异,进而带来隐私问题.现有研究表明:运动传感器能够作为媒介被利用构建侧信道攻击[1],窃取用户的敏感输入[2,3]、获得用户的运动状态[4,5]、识别并追踪特点设备[6−9].更重要的是,基于运动传感器的侧信道攻击易于实现,并且隐蔽性极强.与通话、GPS 等模块不同,当前智能终端架构并没有对运动传感器赋予高等级安全的权限,APP 不需要任何权限即可访问运动传感器[10].恶意程序也可以通过 Web 浏览器[11],或者利用系统漏洞绕过沙盒机制获取传感器数据[12].因此,如何对抗运动传感器的侧信道攻击,是一个非常严重且至关重要的课题.

针对运动传感器侧信道攻击的防护应该同时考虑运动传感器的应用广泛性和侧信道攻击的低门槛特点,需满足可用性、普适性、和灵活性等需求.

1) 可用性:从应用角度来看,运动传感器广泛应用于多样化的 APP,针对侧信道攻击的防御方案不能影响用户使用 APP 时的正常工作流程,不能以牺牲用户体验的方式防御侧信道攻击.
2) 普适性:侧信道攻击的手段和目的多样化,包括泄露敏感输入、特殊用户识别等,防御方案在攻击手段面前应具有普适性.
3) 灵活性:智能终端的硬件和软件定制化程度很高,进而产生很多差异化的操作系统版本,防御方案应该能够尽可能地减少对 APP 和操作系统的修改,同时,应能够在各种操作系统和硬件设备下进行迁移,不应受到实施环境的约束.

尽管研究者提出了很多防御方案[13],现有的防御机制均不能同时满足上述需求.已知防御方案可以分为以下 4 类.

1) 抑制传感器性能.通过降低传感器的采样频率,甚至禁止 APP 访问传感器[14,15]是最直接的对抗侧信道攻击的防御方案,但由于难以区分数据访问的目的,限制传感器性能的解决方案会严重影响 APP 的正常运行,牺牲用户体验,不满足可用性需求.
2) 传感器访问控制.通过 APP 数据流的上下文信息判断是否允许其访问传感器数据[16],但是访问控制无法防御伪装成合法 APP 的恶意攻击,因此普适性存在欠缺.
3) 随机化方案.以最具代表性的系统键盘随机化方案[17]为例,它通过随机化虚拟键盘的布局,破坏传感器数据与用户输入行为之间的映射关系.但是该方案对于以追踪为目的的侧信道攻击无能为力,修改用户已经非常熟悉的键盘布局对于用户体验而言也十分不友好,无法满足可用性和普适性.
4) 传感器数据破坏.文献[18]提出,通过嗅探程序向用户进行敏感操作过程中产生的传感器数据中注入大量噪声,破坏传感器数据可用性.然而注入行为本身破坏了 Android 的安全机制[19],依赖于对特定系统的修改,不具备灵活性需求.

针对上述研究问题,本文提出基于差分隐私 Laplace 机制[20]的传感器信号混淆方案,能同时满足可用性[21]、普适性和灵活性的需求.我们对传感器原始读数进行混淆,设计了运动传感器侧信道防御方案.随后,本文提出了侧信道攻击的理论分析框架,通过分别分析信号混淆对于特征数值、特征分布以及学习模型的干扰过程,论述了本方案的防御原理,论证了本方案对现有环境中几乎所有运动传感器侧信道均具有防御能力.最后,基于 11 种典型侧信道攻击建立防御实验,验证了该防御方案对抗实际攻击的效果.

本文研究的主要贡献如下.

(1) 针对运动传感器侧信道防御不足的问题,揭示了运动传感器侧信道构建的通用模型.同时,提出了一种基于差分隐私的传感器信号混淆防御方案,该方案对攻击者和用户完全透明,在可用性、普适性、

与灵活性上均具有突出表现.

(2) 建立了抗侧信道攻击的防御干扰理论分析框架,结合具体运动传感器侧信道,详细地分析了防御方案干扰侧信道攻击的各种因素以及干扰原理,论证了本文提出的运动传感器侧信道防御方案能够有效对抗符合通用模型的各种类型侧信道攻击.

(3) 对 8 种典型的输入侧信道和 3 种追踪侧信道进行系统的防御实验,验证了本文提出的运动传感器侧信道防御方案在应对实际攻击时的有效性,并对实验现象进行了合理的讨论与分析.

本文第 1 节讨论运动传感器侧信道的通用模型.第 2 节介绍防御方案中的信号混淆方法.第 3 节与第 4 节分别从特征分布、特征数值和学习模型的角度讨论信号混淆对侧信道构建的干扰原理.典型传感器侧信道的防御实验和结果分析在第 5 节中呈现.第 6 节介绍相关工作.第 7 节对本文工作进行总结.

1 运动传感器侧信道模型分析

用户使用移动设备时,设备的空间状态会产生与用户行为相关的改变.例如:当点击手机屏幕某个位置时,手机会受外力的作用而转动,移动设备中的运动传感器能够感应到运动状态的改变,并以不同的形式(加速度、角速度、空间角度等)响应,攻击者能够利用“运动传感器-运动状态-用户行为”之间的映射关系构建侧信道,窃取用户隐私信息.我们把以点击位置为目的的运动传感器侧信道称为“输入侧信道”,以用户运动行为[4,5]为目的的侧信道称为“状态侧信道”.其中,输入侧信道常被用于泄露用户的 PIN(personal identification number)、支付密码、实时聊天内容等隐私信息,具有更强的危害性.

运动传感器还被用于构建“追踪侧信道”.研究结果表明:由于生产厂商、使用年限、物理损坏等因素影响,手机中的传感器具有独特的缺陷,导致实际测量的数据与真实值之间存在符合线性仿射变换的误差,利用该特性能够实现对特定设备的追踪.通过对各种类型侧信道的构建原理和实施过程进行分析,我们发现基于运动传感器的侧信道攻击可以通过相同的模型描述,如图 1 所示.

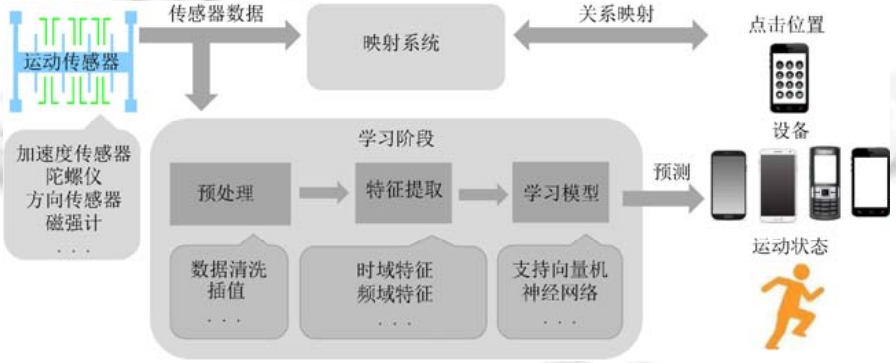


Fig.1 Common pattern of motion sensor-based side-channel attacks

图 1 运动传感器侧信道攻击通用模型

图 1 中,映射系统表示侧信道的利用对象,包含了传感器数据与特定行为或设备之间的映射关系.定义基于传感器读数的特征空间$\chi \subseteq R^n$为 n 维向量的集合,向量的维度 n 依赖于具体侧信道实施方案.用户行为空间由类标记集合$\mathcal{Y}=\{c_1,c_2,\ldots,c_K\}$表示,$c_K$表示可能的行为,例如点击屏幕的某个位置或者某台具体设备.X 是定义在传感器特征空间χ上的随机变量,Y 是定义在用户行为空间$\mathcal{Y}$上的随机变量,则运动传感器侧信道可以看做是用户行为 Y 与传感器特征向量 X 的联合概率分布 $P(X,Y)$,构建侧信道实际上是学习条件概率分布 $P(Y|X)$的过程.运动传感器侧信道的构建包含了数据预处理、特征提取和分类器学习等 3 个阶段,根据侧信道针对的具体目标和实施场景,侧信道选择的传感器类型、特征属性、分类器模型等存在差异.

由上述分析可得:无论哪种类型的运动传感器侧信道,其关键都在于用户行为与传感器之间映射关系 $P(X,Y)$的学习过程[22].因此,可以通过干扰侧信道的学习阶段实现防御.对抗机器学习[23,24]领域中,研究者分别通过

干扰学习模型的训练阶段和预测阶段,有效地降低了机器学习的预测效果.然而,已有的对抗机器学习方法并不适用于运动传感器侧信道防御,主要原因在于:实际环境下,防御框架无法准确区分出侧信道攻击的不同阶段.

针对上述问题,本文结合差分隐私的思想,设计了一种基于传感器读数混淆的防御方案,无差别地向传感器读数中注入少量噪声,具体信号混淆方法将在第 2.2 节介绍.

2 防御机制实施方案

2.1 差分隐私技术

差分隐私是对通过算法消除个人隐私的数学定义,用于在保证一定统计数据精度的情况下,有效确保高度的隐私性.设ε为正实数,A 为一随机算法,A 将数据集作为输入.数据集 D_1 和 D_2 为非单一元素数据集,且 2 个数据集仅相差 1 个元素,若 A 的所有可能输出的子集 S 满足公式(1),则称算法 A 是ε-差分隐私:

$$\Pr[A(D_1)\in S]\leqslant e^{\varepsilon}\times\Pr[A(D_2)\in S] \tag{1}$$

其中,概率取决于算法的随机性.差分隐私中,某个查询函数 f 的敏感度 s 由 f 在 2 个相邻数据集 D_1 和 D_2 上的最大差异$|f(D_1)-f(D_2)|$决定.

Laplace 机制是最常用的差分隐私机制,通过向查询结果中添加受控噪音降低查询结果的准确度.Laplace 噪声的概率密度函数为 $noise(x)\propto\exp(-|x|/\beta)$,$x$ 为概率密度函数中的自变量.在 Laplace 机制下,满足ε-差分隐私的 A 输出副本可以表示为 $f(x)+Lap(s/\varepsilon)$.

差分隐私具有严格的数学证明,能够在最大化攻击者能力的前提下,保证用户的隐私安全.这与侧信道防御场景相似,即假设攻击方能够获得尽可能丰富的用户信息.另一方面,混淆方案的首要前提是尽可能地减少对用户体验的影响,需要随机函数以较高的概率产生低值噪声,例如负指数分布.然而,负指数分布产生的噪声均为正值,进行噪声注入后,所有的特征将向同一个方向进行平移,并不能最大化各类特征区间之间覆盖.因此,由两个不同方向的指数分布背靠背拼接在一起所构成的双指数分布,即 Laplace 分布,更适合进行侧信道学习过程的干扰.通过注入服从 Laplace 分布的随机噪声,某些维度上的统计特征可以近似地看成向正负方向同时进行平移,当各类特征区间接近时,特征样本的覆盖程度将被最大化,更大程度地降低了特征精度.详细的防御原理将在后续两节进行阐述.

此外,相比于相似对称性的高斯分布等常见分布,Laplace 分布具有尖峰的特点.根据我们的研究,少量的噪声足以对侧信道造成显著干扰,为保证数据的可用性和实时性,我们希望得到更多的低值噪声.图 2 展示了相同尺度参数下高斯分布与 Laplace 分布的概率密度函数,由图中能够看出,在输出范围内,Laplace 分布能够以较高的概率输出低值噪声.虽然噪声的数值越高在干扰模型学习能力上越具有优势,但也降低了传感器数据的可用性.而且经实验发现,注入服从高斯分布的噪声会对用户体验产生明显的负面影响.综合考虑差分隐私技术与防御场景需求,本文选择以拉普拉斯分布产生随机噪声.

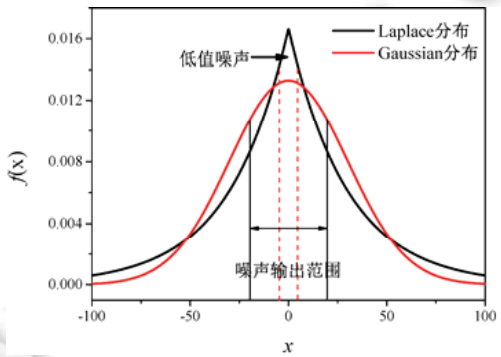


Fig.2 Probability density function

图 2 概率密度函数

将统计特征提取步骤近似地看做查询操作,为运动传感器的每一维(Android 下运动传感器通常包含 3 个维度)的读数实时添加符合 Laplace 分布的随机噪声 $noise\sim Lap(0,\beta_d)$进行信号混淆,其中,

$$\beta_d=\frac{s_d}{\varepsilon/3} \tag{2}$$

s_d 为当前维度 d 的敏感度,其值等于窗口范围内传感器读数的最大值与最小值的差值.混淆因子ε表示信号混淆程度,由 Laplace 的概率分布函数可知:ε越大,概率密度的尺度参数越小,产生高值噪声的概率越大.

2.2 信号混淆方案

相比于合法 APP 中传感器的相关功能,传感器侧信道对数据的精度更加敏感,鲁棒性更低.本文提出的运动传感器侧信道防御方案通过差分隐私中的 Laplace 机制,以随机概率向传感器的当前信号 $x(n)$注入随机噪声 $noise(n)$:

$$x_o(n)=x(n)+noise(n) \tag{3}$$

其中,$x_o(n)$表示混淆后的传感器读数.我们将该方案称之为“平移混淆”,对传感器的响应时间也以相同方式进行混淆.为实现对用户和侧信道攻击方的完全透明,对框架层中的 *android_hardware_SensorManager* 模块进行修改.APP 在应用层实例化 *SensorManager* 对象,重写回调函数 *onSensorChanged*,当传感器检测到设备状态变化时,传感器数据将经由 *android_hardware_SensorManager* 模块向应用层的回调函数反馈.我们在框架层中添加一个缓存对象用于存放底层响应的传感器数据,并实时注入符合 Laplace 分布的受控随机噪声,若随机噪声高于当前读数一定比例,则重新产生随机噪声.信号混淆具体方法可参考我们先前的研究[21].

为了保证合法应用程序中传感器相关功能的正常使用,将噪声的程度控制在一定范围内.然而,运动传感器侧信道对输入数据中的噪声(例如环境中的白噪声)具有一定的鲁棒性,过少的噪声可能难以有效降低侧信道攻击的成功率.此外,由于具体实现方案和攻击场景的差异,基于信号混淆的防御机制能否普适地对抗侧信道攻击有待验证.因此,后续两节中我们将结合具体的输入侧信道和追踪侧信道攻击,分析噪声注入对攻击的干扰原理和影响因素,论证防御机制有效性.

参与研究分析的设备见表 1,其中包含了当前市场上主流手机生产厂商的多种型号设备以及操作系统版本.实验与分析过程中,所有设备的采样频率均为 50HZ.

Table 1 List of devices

表 1 研究设备列表

设备	CPU	系统版本
Meizu m3x	Helio P20	5.0
Meizu max5	Helio X10	4.4
MI 4c	Snapdragon 808	4.4
MI 6	Snapdragon 835	5.0
MI 6x	Snapdragon 660	5.0
MI note3	Snapdragon 650	4.4
Pro 4	APQ 8064	4.1
OPPO R9s	Snapdragon 625	6.0
Huawei P20	Qilin 970	8.1
Galaxy S8	Snapdragon 835	7.0

近年来,虽然指纹、人脸识别等生物认证的研究趋于成熟,但是字符密码、图像密码等依靠用户输入的传统身份认证机制仍然在市场中占主要地位[25].我们筛选出研究领域中具有较大影响力的 8 输入侧信道做为案例进行研究,各个输入侧信道的详细信息见表 2.

参与研究的追踪侧信道见表 3.

Table 2 List of input side channels

表 2 输入侧信道列表

侧信道研究	传感器类型
Accessory[15]	Accelerometer
Signature[26]	Linear-Accelerometer Gyroscope Orientation
Pinlogger[27]	Accelerometer Orientation
Textlogger[28]	Accelerometer Gyroscope
Tapprints[29]	Accelerometer Gyroscope
Taplogger[30]	Accelerometer Gyroscope
Input-extraction[31]	Linear-Accelerometer Orientation
Practicality[32]	Accelerometer

Table 3 List of tracking side channels

表 3 追踪侧信道列表

侧信道研究	传感器类型
MobileTracking[6]	Accelerometer
TrackingExploring[7]	Linear-Accelerometer Accelerometer Gyroscope
AccelPrint[8]	Accelerometer

3 特征影响分析

不同于机器学习中的噪声(标签噪声和输入噪声),直接在传感器读数中注入的混淆噪声具有全局性,即干扰行为同时存在于侧信道的学习和攻击过程.为了验证防御方法在不利环境下的防御性能,假设样本同时具有正确性.由于干扰的全局性特点,侧信道的训练集和预测集中的样本分布会发生同步改变,因此,传统机器学习中的噪声干扰原理在当前场景下并不适用.本节中,我们首先验证数据集的样本分布情况,然后对特征数值受噪声注入的影响状况进行分析.

3.1 特征分布分析

运动传感器侧信道的核心是从已有的数据中学习用户行为与传感器数据之间的映射规律,并对未知的行为做出决策.因此,训练集中的数据应具有较好的总体代表性,即假设训练集与预测集独立同分布.因为噪声的全局性,对于传感器读数的混淆行为并不会对数据集的同分布假设造成影响.

重新定义 X 为原始传感器特征空间中任意维度上的随机变量,Y 为引入噪声后的改变量,Z 为添加噪声后的特征随机变量,易得 X,Y 独立分布.添加噪声可以看做在当前特征维度引入 1 个或多个独立 Laplace 分布的随机变量,而注入行为可以分解为“加、减、乘、除”这 4 种基本操作.

对于加法操作,若(X,Y)的概率密度为 $f(x,y)$,则 $Z=X+Y$ 的分布函数为

$$F_Z(z)=P\{Z\leqslant z\}=P\{X+Y\leqslant z\}=\iint\limits_{x+y\leqslant z}f(x,y)\mathrm{d}x\mathrm{d}y=\int_{-\infty}^{+\infty}\left[\int_{-\infty}^{z-x}f(x,y)\mathrm{d}y\right]\mathrm{d}x \tag{4}$$

所以,Z 的概率密度 $f_Z(z)$为

$$f_Z(z)=F_Z'(z)=\int_{-\infty}^{+\infty}f_X(x)f_Y(z-x)\mathrm{d}x \tag{5}$$

通过加法添加噪声后,训练集与预测集之间保持相同分布,分布函数由噪声分布和原始特征分布共同决定.同理可得,减法操作 $Z=X-Y$ 的概率密度函数为

$$f_Z(z)=F_Z'(z)=-\int_{-\infty}^{+\infty}f_X(x)f_Y(x-z)\mathrm{d}x \tag{6}$$

对于乘法操作,$Z=XY$ 的分布函数可以表示为

$$\left.\begin{aligned} F_Z(z) &= P\{XY \leqslant z\} \\ &= P\left\{Y \geqslant \frac{z}{X}, X<0\right\} + P\left\{Y \leqslant \frac{z}{X}, X>0\right\} + F_X(0) \\ &= \int_{-\infty}^{0}\left(\int_{\frac{z}{X}}^{+\infty} f_Y(y)\mathrm{d}y\right) f_X(x)\mathrm{d}x + \int_{0}^{+\infty}\left(\int_{-\infty}^{\frac{z}{X}} f_Y(y)\mathrm{d}y\right) f_X(x)\mathrm{d}x + F_X(0) \end{aligned}\right\} \tag{7}$$

新的特征随机变量 Z 的概率密度 $f_z(z)$为

$$f_Z(z) = F_Z'(z) = \int_0^{+\infty} F_Y\left(\frac{z}{X}\right) f_X(x)\mathrm{d}x - \int_{-\infty}^{0} F_Y\left(\frac{z}{X}\right) f_X(x)\mathrm{d}x = \int_{-\infty}^{+\infty} f_Y\left(\frac{z}{x}\right) f_X(x)\frac{1}{|x|}\mathrm{d}x \tag{8}$$

同理,以除法形式添加噪声的新特征变量 $Z=X/Y$ 的分布函数可以表示为

$$\left.\begin{aligned} F_Z(z) &= P\left\{\frac{Y}{X} \leqslant z\right\} \\ &= P\{Y \geqslant zX, X<0\} + P\{Y \leqslant zX, X>0\} \\ &= \int_{-\infty}^{0}\left(\int_{zx}^{+\infty} f_Y(y)\mathrm{d}y\right) f_X(x)\mathrm{d}x + \int_{0}^{+\infty}\left(\int_{-\infty}^{zx} f_Y(y)\mathrm{d}y\right) f_X(x)\mathrm{d}x \end{aligned}\right\} \tag{9}$$

除法操作后,特征随机变量 Z 的概率密度为

$$f_Z(z) = F_Z'(z) = \int_{-\infty}^{+\infty} f_Y(xz) f_X(x)|x|\mathrm{d}x \tag{10}$$

因此可知:混淆后的新特征集服从与随机噪声相关的概率分布,侧信道训练集和测试集之间仍然满足独立同分布的假设.

3.2 特征数值分析

由第 1 节可知,运动传感器侧信道的学习阶段需要从传感器读数中提取统计特征构造特征向量.特征值受到噪声信号的具体影响依赖于统计方法以及特征的空间分布.以时域和频域下典型特征为例,讨论噪声对于特征数值的影响.

首先,随机噪声符合期望为 0 的 Laplace 分布,当传感器读数的长度足够时,平移混淆方法对于平局值、均差等特征产生很小的影响.设当前传感器的某个维度上的信号序列长度为 n:$\{X_i\}$:=$x_1,x_2,\ldots,x_n$,则时域中均值 M 特征值描述为

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{11}$$

设传感器读数 x_i 处以平移混淆方式注入随机噪声,则混淆后的样本平均值可以表示为

$$\overline{x}_o = \frac{1}{n}\sum_{i=1}^{n}(x_i + noise_i) = \frac{1}{n}\sum_{i=1}^{n} x_i + \frac{1}{n}\sum_{i=1}^{n} noise_i = \overline{x} \tag{12}$$

由公式(12)得,平移混淆并不会影响侧信道的平均值特征.类似地,经过混淆后的时域均差 D 特征为

$$D_{\overline{x}}^{o} = \frac{1}{n}\sum_{i=1}^{n}|x_{oi} - \overline{x}_o| = \frac{1}{n}\sum_{i=1}^{n}|x_i - \overline{x}_o + noise_i| \tag{13}$$

考虑噪声数值的符号,上式可以表示为

$$D_{\overline{x}} - \frac{1}{n}\sum_{i=1}^{n}|noise_i| \leqslant D_{\overline{x}}^{o} \leqslant D_{\overline{x}} + \frac{1}{n}\sum_{i=1}^{n}|noise_i| \tag{14}$$

在混淆程度较小的情况下,小数值噪声的出现概率更大,噪声的均值更小,均差特征受到噪声的影响有限;随着混淆程度增大,均差特征被干扰的程度随之增加.注入噪声对于非线性统计的特征具有更明显的影响.以时域下标准差σ与均方根 R 为例,经平移混淆后,传感器读数序列的标准差特征σ_o表示为

$$\sigma_o = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_{oi} - \overline{x}_o)^2} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2 + \frac{1}{n}\sum_{i=1}^{n}(2(x_i - \overline{x}) \times noise_i + noise_i^2)} \neq \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2} = \sigma \tag{15}$$

经平移混淆后的均方差属性 R_o 为

$$R_o=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_{oi})^2}=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i)^2+\frac{1}{n}\sum_{i=1}^{n}(2x_i\times noise_i+noise_i^2)}\neq\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i)^2}=R \tag{16}$$

由公式(15)和公式(16)得:平移混淆会对标准差、均方根等非线性统计特征产生较大影响,影响程度依赖于传感器读数序列以及随机噪声强度.在实际数据集中,通过对已知传感器侧信道中时域特征进行统计得出:平移混淆下,特征随混淆因子增大而呈现非下降趋势(上升或保持),其中包括了极值、方差等常用特征,以及偏斜度、峰度、相关系数等非常用特征.以平均值、标准差和均差特征为例,图 3 展示了 3 种特征受平移混淆的影响差异,特征提取自线性加速度 x 方向.图中横坐标表示对传感器信号的混淆程度,纵坐标表示特征的数值.可以看出,与上述分析结果一致:均值特征基本不受添加噪声的影响;均差的影响随混淆影子的增加而呈现线性增长;受到混淆影响最大的为均方差特征,干扰呈现指数型上升.

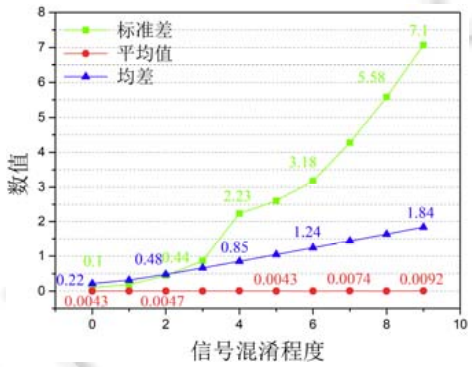


Fig.3 Value changes of time domain features of linear acceleration in x direction under different levels of translating obfuscation

图 3 不同程度平移混淆下线性加速度 x 方向上时域特征数值变化

某些输入侧信道[31]和追踪侧信道[7]会提取频域特征作为时域特征的扩充,攻击者将传感器产生的信号序列作为离散的信号,并通过离散傅里叶变换得到信号的频域表示$\{X_k\}:=X_0,X_1,\ldots X_{N-1}$,其中,

$$X_k=\sum_{n=0}^{N-1}x_n\cdot e^{-j2\pi kn/N}=\sum_{n=0}^{N-1}x_n\cdot[\cos(2\pi kn/N)-j\cdot\sin(2\pi kn/N)] \tag{17}$$

设传感器读数序列的离散傅里叶变换为 $X(\omega)$,噪声序列 $noise(n)$的离散傅里叶变换为 $Noise(\omega)$,其中,$\omega=e^{j2\pi/N}$,则根据离散傅里叶变换的线性特性可得:

$$x(n)+noise(n)\xleftrightarrow[IDTF]{DTF}X(\omega)+Noise(\omega) \tag{18}$$

由公式(18)可知,平移混淆对传感器数据频域的影响仅与引入的时域噪声相关.时域噪声信号在时间轴上服从随机分布,因此,频域噪声信号的分布与时域噪声分布无直接关系.当混淆程度较小时,时域上的噪声难以改变原始信号的变化趋势,平移混淆在信号频域上的干扰主要体现在高频部分;随着混淆因子的增大,信号的低频部分也会出现明显的干扰.图 4 显示了频域中,点击按键“1”时产生的 x 维度上加速度信号受混淆因子ε=5 平移混淆的影响情况,图中横坐标表示频率,纵坐标表示幅度.

可以看出,由于 $Noise(\omega)\geqslant 0$,信号幅度在所有频率上均会产生非零增长.因此,基于频域提取的绝大部分特征都会受到信号混淆的影响.

以标准差特征为例,设样本在频域的标准差为σ_s,进行平移混淆后,频域标准差改变为

$$\sigma_s^o=\sqrt{\left(\sum_{k=0}^{N-1}(k+1)^2\cdot(X_k+Noise_k)\right)\Big/\left(\sum_{k=0}^{N-1}(X_k+Noise_k)\right)} \tag{19}$$

由公式(19)得:频域标准差特征的改变程度与原始信号及噪声信号相关,噪声信号的高频干扰对于频域标

准差特征的影响更大.

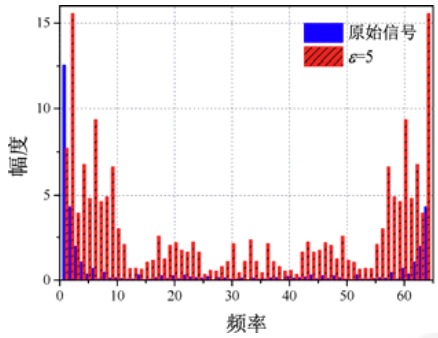


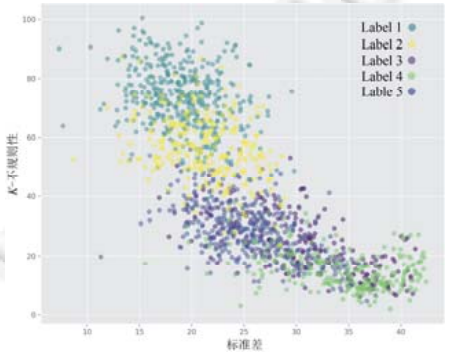
Fig.4 Impact on frequency signal of acceleration in x direction with obfuscation level ε=5

图 4 混淆程度ε=5 的平移混淆对于加速度 x 维度上频域信号影响

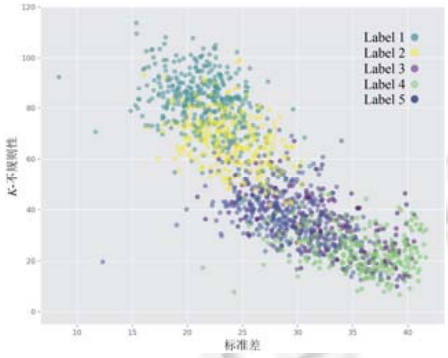
考察 *K*-不规则性特征 IK_s:

$$IK_s^o=\sum_{k=1}^{N-2}\left|X_k-\frac{X_{k-1}+X_k+X_{k+1}}{3}-\frac{2Noise_k-Noise_{k-1}-Noise_{k+1}}{3}\right|\neq\sum_{k=1}^{N-2}\left|X_k-\frac{X_{k-1}+X_k+X_{k+1}}{3}\right|=IK_s \tag{20}$$

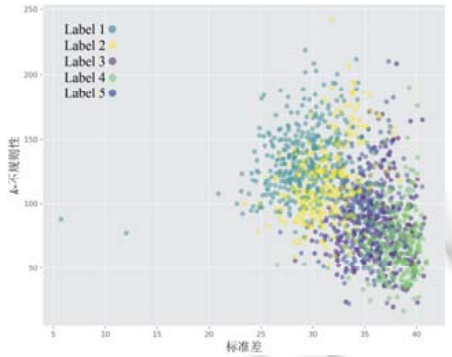
K-不规则性的改变量仅与噪声在频域的分布有关.图 5 直观地展现了平移混淆对于频域标准差和 *K*-不规则性特征的影响情况,其中,混淆因子$\varepsilon\in\{0,1,5,9\}$,特征提取自点击按键“1”,“3”,“7”,“9”,“0”这 5 类事件对应的加速度 *x* 维度上的信号.



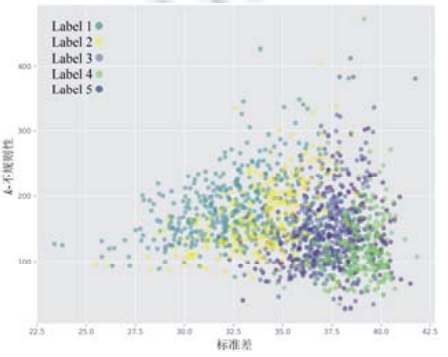
(a) *x* 方向初始加速度 2 维频域特征分布



(b) 混淆程度ε=1 时 *x* 方向加速度 2 维频域特征分布



(c) 混淆程度ε=5 时 *x* 方向加速度 2 维频域特征分布



(d) 混淆程度ε=9 时 *x* 方向加速度 2 维频域特征分布

Fig.5 Impact on frequency features *K*-regularity and std deviation with obfuscation level $\varepsilon\in\{0,1,5,9\}$

图 5 混淆程度$\varepsilon\in\{0,1,5,9\}$的平移混淆对频域 *K*-不规则性与标准差影响情况

图 5 中,横坐标表示样本的频域标准差特征,纵坐标表示 *K*-不规则性特征.混淆因子较小时(图 5(b)),平移混淆对于传感器信号频域的干扰有限,标准差和 *K*-不规则性没有出现明显的变化;混淆因子增大后,2 类特征的改变程度逐渐增强(图 5(c)、图 5(d)).此外,由于噪声信号在时间上具有随机性,频域特征的改变没有稳定趋势.

综上所述,传感器读数有限的情况下,平移混淆会导致绝大部分统计特征产生改变,各类特征由于提取方法的差异,受平移混淆的影响程度存在明显差异.混淆行为对时域特征的影响与噪声的概率分布相关,但在频域特征上的影响无明显规律性.根据机器学习原理,特征对于学习的贡献能力各异,因此,上述结果必然影响模型的预测.

4 模型干扰分析

本节将从学习模型的角度分析信号混淆对抗运动传感器侧信道可能存在的影响因素.信号混淆对于输入侧信道和追踪侧信道的物理意义不同,且攻击场景存在很大差异,因此分别讨论输入侧信道和追踪侧信道下的模型受影响情况.

4.1 输入侧信道模型干扰分析

研究[33]表明:当点击手机屏幕时,用户具有独特的行为习惯(敲击力度、时间间隔等),输入侧信道中,待预测类别之间仅存在由于点击位置不同而产生的微弱行为差异.同时,手机屏幕的尺寸进一步限制了行为差异,这些因素反应在特征空间上表现为各个类别之间的边界模糊.

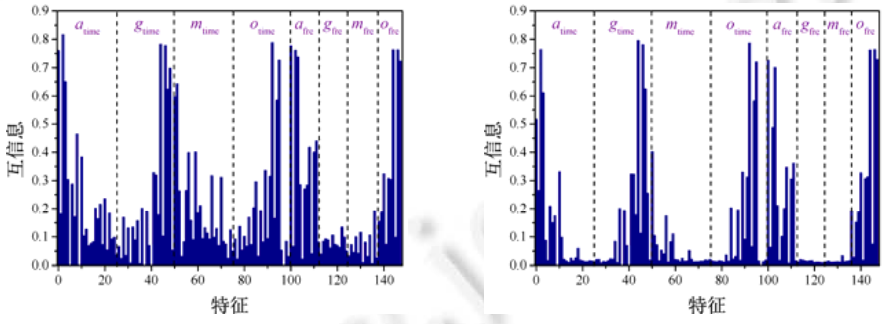
4.1.1 特征区分度分析

信号混淆可以被近似地看作对传感器数据进行平移,根据第 3 节中的分析结果,混淆操作对特征的影响差异性可能导致类别之间的混叠程度增加,降低各类别的区分度,使得类别之间的边界变得更加模糊.

我们通过互信息(mutual information,简称 MI)[34]描述各维度上特征在特征空间中的区分度,互信息定义为

$$MI(U,V)=\sum_{i=1}^{|U|}U\left|\sum_{j=1}^{|V|}V\right|\frac{|U_i\cap V_j|}{N}\log\frac{N|U_i\cap V_j|}{|U_i||V_j|} \tag{21}$$

其中,*U*,*V* 分别表示 *k*-means 聚类和真实聚类,|·|表示当前类别中的样本数量.首先记录传感器在用户输入过程中产生的加速度 *a*、角速度 *g*、方向角度 *o* 和磁强 *m* 信号,根据数字键盘布局分为 10 个类别,分别提取已知输入侧信道中共同的典型时域和频域特征,对各个维度的特征计算互信息,结果如图 6(a)所示,其中,横坐标表示具体特征类型,纵坐标表示对应特征的互信息值.



(a) 典型特征互信息 (b) 混淆程度 ε=5 时典型特征互信息

Fig.6 Mutual information of typical time and frequency features of 4 motion sensors' readings

图 6 4 类运动传感器数据的典型时域和频域特征互信息

从图 6(a)中可以看出,不同传感器下的特征之间互信息分布存在明显差异,说明各种类型的运动传感器对于输入行为具有特殊的映射形式.此外,相同传感器下的不同特征之间的区分度差异较大,例如,时域上最大值(Max)的互信息约为 0.76,而最小值(Min)的互信息值只有 0.18 左右.对传感器信号进行混淆因子 ε=5 的信号混

淆,再次计算每个特征维度的互信息,结果如图 6(b)所示.比较图 6 子图,信号混淆后的数据集中,部分特征的互信息降低,表明特征在对应维度上的混叠程度增加.

特征区分度的改变会影响逻辑回归、决策树等学习模型,这些模型通过寻找最优决策边界的方式,构建空间判别类域.根据对已有侧信道研究的统计,决策树与逻辑回归模型都属于运动传感器侧信道的最佳学习模型,因此,类别之间区分度的降低是信号混淆能够抵抗输入侧信道的可能原因之一.

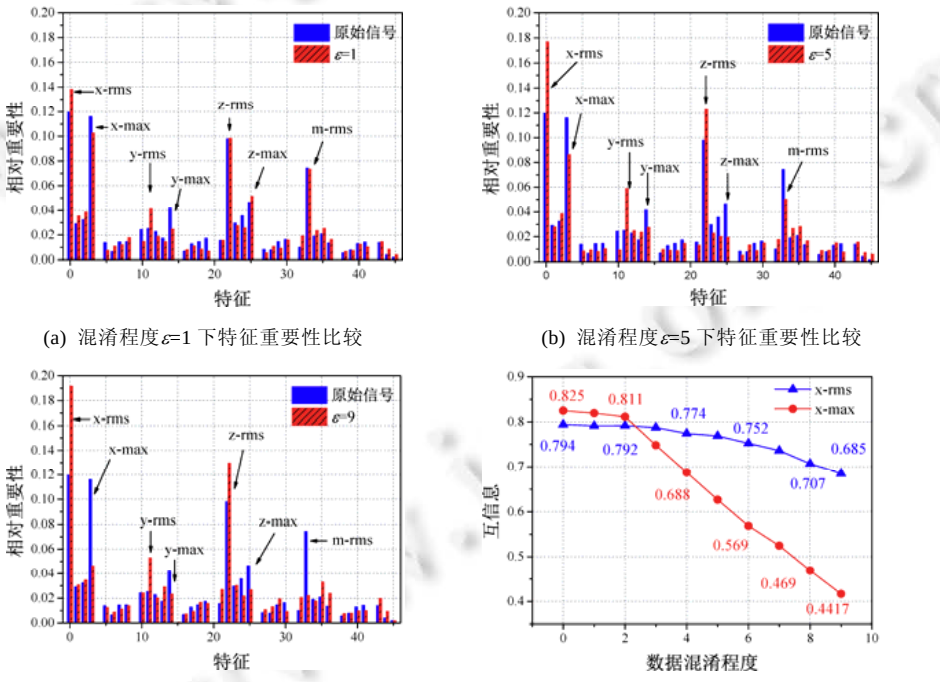
以决策树模型为例,讨论区分度对输入侧信道的影响过程.决策树以重要性描述特征之间的相对区分度.设当前样本集合 D 中具有 y 类样本,$p_k(k=1,2,\ldots,y)$为集合中第 k 类样本所占的比例,集合 D 进行决策的信息熵表示为

$$Ent(D)=-\sum_{k=1}^{y}p_k\log_2 p_k \tag{22}$$

以信息增益作为节点划分准则,设特征向量中的连续属性 a 有 n 个可能取值,并按大小排序$\{a^1,a^2,\ldots,a^n\}$,t 为属性 a 的划分点,D 可以被划分为 D_t^- 与 D_t^+,将相邻区间$[a^i,a^{i+1}]$的中位点作为候选划分点,考察包含 $n-1$ 个元素的候选划分点集合 $T_a=\{(a^i+a^{i+1})/2|1\leqslant i\leqslant n-1\}$,则连续属性 a 对样本集 D 进行划分所获得的信息增益为

$$Gain(D,a)=\max_{t\in T_a}Gain(D,a,t)=\max_{t\in T_a}Ent(D)-\sum_{\lambda\in\{-,+\}}\frac{|D_t^\lambda|}{|D|}Ent(D_t^\lambda) \tag{23}$$

$Gain(D,a,t)$是 D 基于划分点 t 二分后的信息增益,信息增益越大,a 确定的情况下对于当前剩余样本分类的重要性越强.由于节点使用连续属性划分后,后续节点依然可以使用相同属性进行划分,因此,相对重要性更强的关键特征将会主导模型的学习预测走向[35].若决策树中相对重要性高的特征的实际区分度降低,则模型的整体预测能力差.Accessory 侧信道利用决策树模型学习传感器信号特征,提取加速度 3 个维度上加速度传感器数据和欧几里得级数的时间域统计特征,构建输入侧信道.混淆因子$\varepsilon\in\{0,1,5,9\}$时,决策树训练阶段各个特征的重要性变化过程如图 7 所示.



(a) 混淆程度ε=1 下特征重要性比较　(b) 混淆程度ε=5 下特征重要性比较

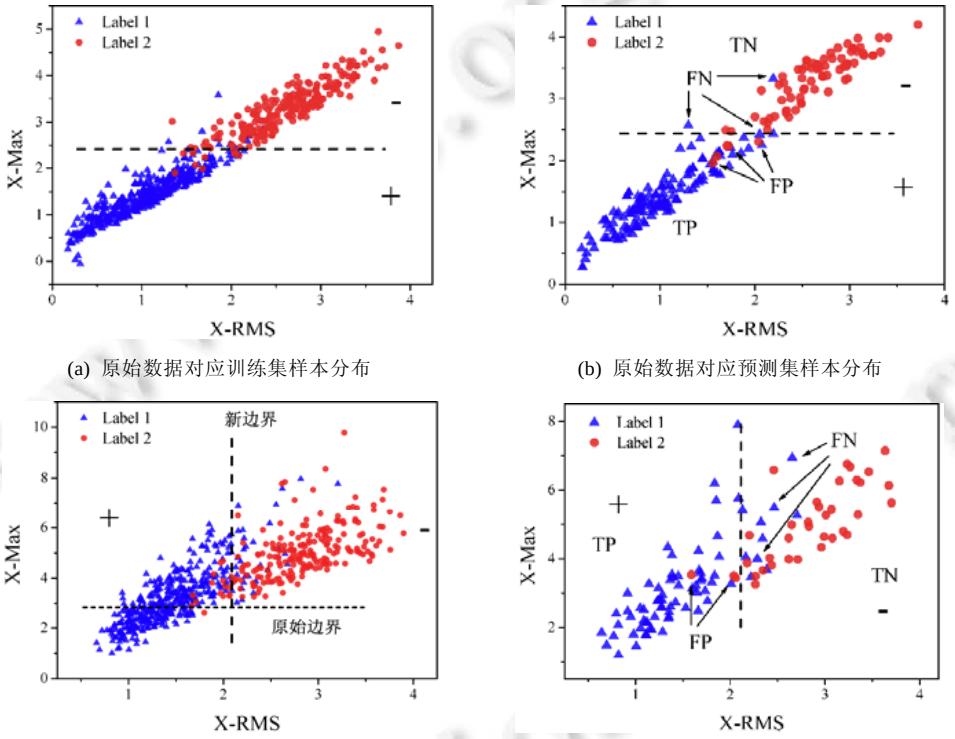
(c) 混淆程度ε=9 下特征重要性比较　(d) 多种混淆程度下 RMS 和 Max 特征互信息值变化

Fig.7 Impact on translating obfuscation on feature importance of decision tree model

图 7 平移混淆对决策树模型的特征重要性影响

图 7(a)~图 7(c)中显示了不同混淆因子下各类特征的相对重要性,横坐标表示侧信道中的特征类型,纵坐标表示相对重要性.平移混淆对于不同特征重要性的影响情况各异:原始特征向量中相对重要性较小的特征在注入噪声后的数据集中依旧保持低区分度;传感器 3 个维度上的均方根 *RMS* 和最大值 Max 受到平移混淆的影响较为明显,其中,均方根的相对重要性随混淆程度增加而增强,最大值呈现相反趋势.图 7(d)中显示了传感器 *x* 方向上均方根和最大值的互信息变化情况,2 类特征在对应维度上的区分度均随混淆程度的增大而降低.最大值特征在模型中的相对重要性降低,同时区分度也降低,因此,该特征不会为模型做出有利贡献;均方根特征逐渐主导模型预测,但是该特征的互信息呈下降趋势,各混淆程度下的区分度均低于原始数据集中最大值的区分度,最终导致侧信道攻击准确率下降.

我们分别随机抽取了训练集和测试集中部分样本特征,比较信号混淆前后的实际分布情况,如图 8 所示.对比图 8(a)和图 8(c),平移混淆使得样本在对应维度上的混叠程度增加,同类样本点之间的分布分散.原始数据集下最大值特征的相对重要性较高,因此决策边界垂直于纵坐标方向;经过平移混淆后(图 8(c))最大值特征的区分度急剧下降,均方根获得了相对更高的重要性,决策边界垂直于均方根所在的横坐标方向.然而,此时均方根的区分度不及原始数据中最大值的区分度,新决策边界两侧出现了更多的错误类别.



(a) 原始数据对应训练集样本分布 (b) 原始数据对应预测集样本分布

(c) 混淆程度ε=9 数据对应训练集样本分布 (d) 混淆程度ε=9 数据对应预测集样本分布

Fig.8 Distribution of maximum and root mean squre in training set and prediction set with obfuscation level $\varepsilon\in\{0,9\}$

图 8 混淆程度$\varepsilon\in\{0,9\}$平移混淆下训练集与预测集中最大值和均方根分布情况

定义样本“1”正例,样本“9”反例,上述侧信道的分类结果的混淆矩阵见表 4.其中,*TP*,*FP*,*TN*,*FN* 分别表示真正例、假正例、真反例、假反例的样例数.正例的查准率 P_p 和反例的查准率 P_n 表示为

$$P_p=\frac{TP}{TP+FP},P_n=\frac{TN}{TN+FN} \tag{24}$$

由于主导决策边界的特征区分度变低,预测集中(后文图 10(d))中的假正例 *FP* 和假反例 *FN* 增加,真正例 *TP*

和真反例 TN 数量减少,即$\Delta FP,\Delta TN\leqslant 0$,经混淆后的查准率 P_p^o 改变为

$$P_p^o=\frac{TP+\Delta TP}{TP+\Delta TP+FP+\Delta FP}\leqslant\frac{TP+\Delta TP}{TP+\Delta TP+FP}\leqslant\frac{TP}{TP+FP}=P_p \tag{25}$$

同理得 $P_p^o\leqslant P_n$,侧信道的攻击成功率下降.此外,由于平移混淆导致特征之间混叠程度增加,侧信道学习过程变得复杂,注入噪声增加了过拟合的风险,攻击泛化性降低.

Table 4 Confusion matrix of prediction result

表 4 预测结果混淆矩阵

真实类别	预测类别	
	样本 1	样本 9
样本 1	*TP*	*FN*
样本 9	*FP*	*TN*

我们在频域特征中进行同样的实验,并得到了相似的结果.由上述实验分析可以得:平移混淆能够通过降低特征之间区分度的方式,对抗基于空间判别类域的输入侧信道攻击.综上所述,各维度上特征之间区分度的降低是信号混淆方案抑制输入侧信道攻击的原因之一.

4.1.2 特征值域分析

研究过程中发现:当使用 *t*-SNE(*t*-distributed stochastic neighbor embedding)算法[36,37]对特征样本进行降维后,未经信号混淆的原始数据中,各个类别之间无法从视觉上进行区分.然而对所有特征进行归一化后再进行降维,各个类别之间出现了明显的边界.因此可以猜测:原始特征向量中可能存在的数值值域较大但区分度低的属性,进而导致降维后各个类别之间难以划分.

因同样以特征间距离描述相似性,*k*-NN 等模型的分类效果也会受到特征值域影响.不同于决策树等模型,*k*-NN 不具备伸缩不变性.根据第 3.2 节和第 4.1.1 节,添加噪声导致某些特征的值域扩大,并且降低特征的区分度,因此,信号混淆可能通过增大低区分度特征的值域方式,主导侧信道偏向错误预测方向.我们对经平移混淆的数据集进行离差归一化(min-max normalization),重新通过 *k*-NN 构建 Accessory 侧信道,实验结果如图 9 所示.

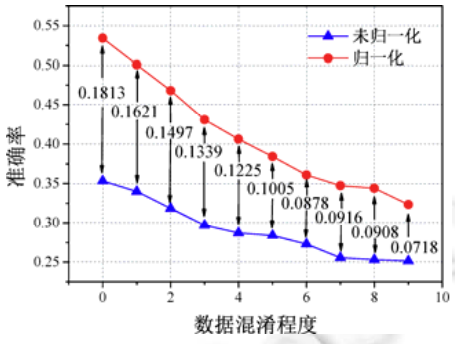


Fig.9 Impact of normalization on prediction accuracy of single tap position of Accessory side channel

图 9 归一化对于 Accessory 侧信道单次点击预测准确率的影响

图 9 中,圆点表示 Accessory 侧信道在归一化后的混淆数据集中预测准确率,三角形表示侧信道在未归一化数据集中结果.相同混淆程度下,归一化能够有效提高 Accessory 侧信道攻击准确率,说明特征向量中始终存在具有大值域、低区分度的特征.随着混淆因子的增大,归一化的效果逐渐降低,混淆因子ε=0 时,归一化提高了 Accessory 单点预测准确率约 18 个百分点;混淆因子ε=9 时,提升的准确率只有约 7 个百分点.高混淆程度下,注入大数值噪声的概率增加,归一化导致特征精度丢失.假设归一化能够完全去除特征数值范围的影响,那么归一化后提高的准确率近似地等于特征值域对侧信道的影响能力,因此可以得出结论:平移混淆导致特征值域改变并不是侧信道攻击受到抑制的原因.

我们在其他输入侧信道的验证中得到了相似的结果.综上所述,输入侧信道的特征向量中,存在具有较大值域且区分度低的特征,引导 *k*-NN 等不具备伸缩不变性的模型的预测方向.然而,特征值域的影响在平移混淆中随混淆程度的增长而降低,所以信号混淆虽然会导致特征的值域改变,但并不是输入侧信道攻击受到抑制的主要原因.

4.2 追踪侧信道模型干扰分析

追踪侧信道基于传感器存在独特误差的背景,运动传感器由硬件缺陷产生的误差服从一次线性仿射变换,平移混淆可以理解为干扰传感器读数的偏移误差.图 10 描述了平移混淆方案对传感器读数的影响意义.图 10 中,横坐标轴表示传感器某一方向的真实信号,纵坐标轴表示该方向上的读取信号,红色实线与蓝色实线分别表示设备 1 与设备 2 的传感器线性误差关系.假设初始环境下,传感器读数完全符合误差假设,2 台设备只有在极小范围内(图 10 中圆圈范围)无法通过误差关系进行区分,我们称该范围“设备盲区”.通过平移混淆注入随机噪声后,真实值与读数之间的线性误差关系在纵坐标方向上发生了平移,误差关系在图 10 中虚线区域内波动,设备盲区扩大到图中阴影部分.

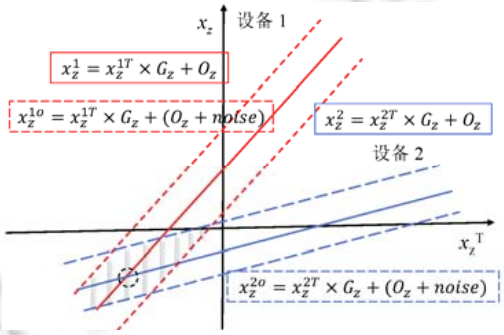
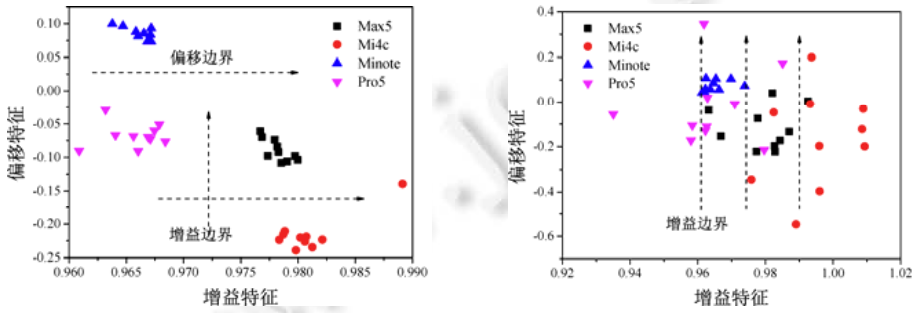


Fig.10 Interference principle of data obfuscation for tracking side channel

图 10 数据混淆对追踪侧信道的干扰原理

4.2.1 特征区分度分析

误差特征是追踪侧信道的基础,因此,误差的区分度在一定程度上决定了追踪侧信道的攻击效果.追踪侧信道攻击场景中,设备与设备之间传感器硬件差异明显,通常情况下,不同设备传感器的偏移特征和增益特征具有很高的辨识度.FingerPrint[38]侧信道通过偏移特征与增益特征构建 2 维特征向量,实现对设备的识别.从表 1 实验设备中随机选择 4 台设备,计算加速度传感器在 *z* 方向的增益特征和偏移特征,重力加速度 g=9.7936 为实验地点的重力加速度,二维特征空间分布如图 11(a)所示.



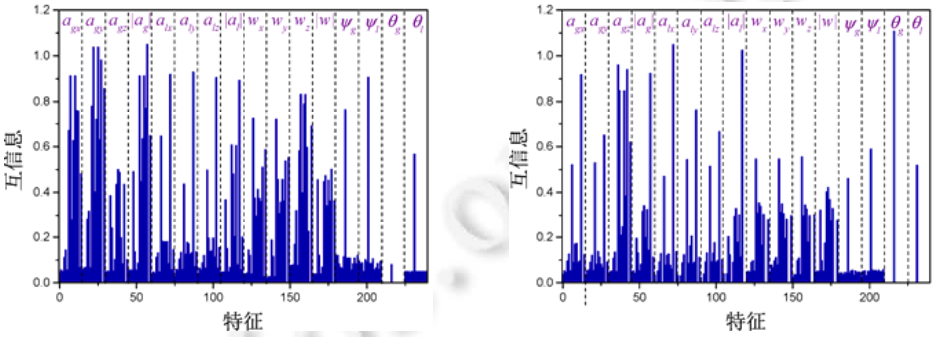
(a) 原始加速度的增益误差与偏移误差分布 (b) 混淆后加速度增益误差与偏移误差分布

Fig.11 Impact on hardware error of accelerometer by data obfuscation with ε=1

图 11 ε=1 数据混淆对加速计硬件误差影响情况

从图 11(a)中能够看出,不同设备的线性误差在增益特征与偏移特征维度上均具备良好的区分度,特征向量在2维特征空间中分布清晰,仅从视觉上就能够精确地识别设备类型.对数据集分别进行混淆因子ε=1的平移混淆后,特征分布如图 11(b)所示.平移混淆导致设备误差关系的盲区变大,不同设备样本之间在特征空间中出现了重叠,区分度下降.理论上,干扰传感器间的误差关系的行为将直接影响从传感器读数中提取的其他特征.

我们在实验数据集中加速度(包含重力影响)和线性加速度中提取了表3中3类追踪侧信道所涉及的共240类特征计算互信息,结果如图 12(a)所示.追踪侧信道中设备之间的差异性明显,大部分特征具有很高的分区度.对上述实验数据集进行混淆因子ε=1 的平移混淆后,再次计算各特征的互信息,结果如图 12(b).除极个别特征以外,信号混淆使得追踪侧信道中大部分特征的区分度降低,高区分度特征的数量有所下降.总体而言,特征的平均区分度远低于未混淆数据集特征下区分度.



(a) 初始 240 类特征互信息 (b) 信号混淆后 240 类特征互信息

Fig.12 Impact on mutual information of typical tracking side channels' features by data obfuscation with ε=1

图 12 典型追踪侧信道特征互信息受ε=1 数据混淆影响

追踪侧信道的重要性实验结果与输入侧信道重要性实验相似,不再重复讨论.综上所述,信号混淆行为通过破坏传感器读数误差关系,影响基于传感器读数的各类特征区分度,进而实现对追踪侧信道攻击的防御.

4.2.2 特征值域分析

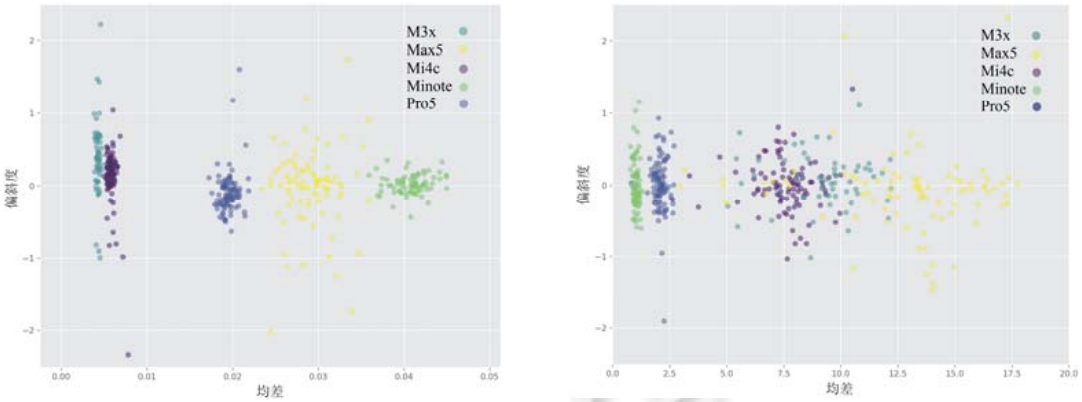
本节中讨论特征值域改变对于追踪侧信道的影响情况.与输入侧信道特征向量类似,追踪侧信道的特征向量中同样存在低区分度、大数值的属性.通过对特征样本进行归一化处理,能够使得进行 *t*-SNE 降维后的各类别之间辨识度提高,不同设备之间将会呈现清晰的聚类结果.

为了探究平移混淆对特征值域以及不具备伸缩不变性学习模型的影响,我们拆分 3 种输入侧信道特征向量中的时域特征和频域特征,枚举所有可能的特征组合,并通过 *k*-NN 进行学习.实验发现:当其他特征与偏斜度等个别特征组合时,模型的预测能力随信号混淆的引入出现明显波动.偏斜度是对传感器数据分布偏斜方向及程度的度量,由于追踪侧信道的攻击场景中所有传感器数据均在设备静止平放时收集,导致偏斜度接近.进一步分析发现:在未经混淆的特征中,偏斜度具有远超其他特征的值域,能够主导模型的预测结果.偏斜度与均差在平移混淆下的分布情况如图 13 所示.

图 13(a)为原始数据集中偏斜度和均差特征的分布情况,均差特征维度上(y 方向),不同设备之间区分度明显;而偏斜度特征维度上(水平方向),各类样本重叠率非常高.观察特征的值域,均差虽然具有较高的区分度,但其值域仅为[0,0.05],远远低于偏斜度的值域[−3,3],因此,模型的表现受到偏斜度特征的主导.对数据集进行混淆因子ε=1 的平移混淆后(图 13(b)),偏斜度的值域并没有受到信号混淆的影响,然而均差的值域改变为[0,20],模型的主导特征由偏斜度转变为具有较高区分度的均差,侧信道的预测准确率反而提升.

将偏斜度这一类具有大值域且区分度低的特征归一化后,以 *k*-NN 构建的 MobileTracking,Tracking Exploring 和 AccelPrint 侧信道在原始数据集中准确率分别提高至 98.4%,97.1%,98.9%.考虑实际侧信道攻击时,攻击者如果通过归一化提高侧信道攻击能力,则帮助消除了特征值域的影响,信号混淆能够有效抵抗追踪侧信

道,若攻击者未进行数据预处理,则侧信道的攻击能力较差,即便信号混淆可能导致攻击准确率出现略微提高,但仍然不足以造成威胁.



(a) 未混淆数据中 2 维特征分布 (b) ε=1 信号混淆后 2 维特征分布

Fig.13 Impact on the distributions of skewness and average deviation by translating obfuscation

图 13 平移混淆对偏斜度特征和均差特征的分布影响

根据以上原理分析可以得出:基于信号混淆的防御方案在对抗输入侧信道和追踪侧信道时,主要通过降低特征之间区分度、增加混叠程度的方式实现侧信道防御.理论上,由于传感器侧信道攻击中需要识别的类别之间边界接近,因此即使低程度的信号混淆也能够影响攻击的成功率,并且该防御方法对于符合运动传感器侧信道通用模型的攻击均有效.

5 运动传感器侧信道防御验证

5.1 输入侧信道防御验证

本节对表 2 中 8 种输入侧信道进行传感器信号混淆防御实验.实验数据收集于 15 位参与者,分别覆盖了多个年龄段与性别.实验中,因为数据集改变后实际最优分类器可能与文献中使用的建议分类器不符,所以首先通过不同的机器学习模型构建侧信道,找出上述侧信道在当前数据集下最合适的分类器模型.各输入侧信道在本文数据集下的分类器模型比较结果见表 5.

Table 5 Impact of learning model on experimental input side channels (%)

表 5 实验环境下学习模型对输入侧信道的影响 (%)

输入侧信道	学习模型					
	SVM	决策树	随机森林	k 邻近	贝叶斯	逻辑回归
Accessory	40	53	**63**	34	55.8	61.7
Signature	17.6	54.3	**68.4**	43.7	34.3	45.8
Pinlogger	18.2	53.1	**64.6**	40.2	28.1	43.7
Textlogger	64.1	58.1	68	48.3	63.4	**75.1**
Tapprints	28.8	59.1	71.5	55.4	63.7	**71.8**
Taplogger	29.3	23.4	26.9	29.5	23.6	**32.6**
Input-extraction	45.6	47.9	**64.6**	59.2	45.8	61.1
Practicality	12	92	**94.5**	43.9	10.3	19.7

表 5 中,除 Practicality 侧信道外,准确率均表示侧信道预测 10 类点击位置(数字键 0~9)的单次预测情况.Practicality 侧信道攻击的对象为完整的输入序列,因此准确率表示对 10 种 6 位长度输入序列的单次预测结果.在当前数据集下,逻辑回归模型与随机森林模型的表现情况相对较好,部分输入侧信道使用 k-NN 模型也能达到较高的预测准确率.

下一步,利用平移混淆对传感器原始数据集进行信号混淆,从中随机选取训练集与测试集进行 50 次重复实验,取实验结果的均值作为最终结果.为避免学习模型干扰,我们选取上述 6 种学习模型中表现最好的 4 类模型分别构造 8 种输入侧信道.表 6 为各输入侧信道分别在混淆因子$\varepsilon\in\{0,1,2,3,4,5,6,7,8,9,10\}$的平移混淆下单次点击预测准确率分布情况.

Table 6 Results of defense experiment against input side channel by translating obfuscation (%)

表 6 平移混淆对抗输入侧信道实验结果 (%)

输入侧信道	ε											
	0	1	2	3	4	5	6	7	8	9	10	学习模型
Accessory	**63**	**59.5**	**56.6**	**52.8**	**48.4**	**47.2**	**47.1**	**43.8**	**40.7**	**40.9**	**39.3**	随机森林
	53	50.1	49.2	45.9	43.8	42	40.1	38.8	37.3	36.3	34.7	决策树
	34	32.7	32.2	30.1	29	27.7	26.9	25.1	25	23.5	22.5	*k* 邻近
	61.7	57	54.3	51.8	50.7	49.4	48.1	47.1	45.5	44.6	57	逻辑回归
Signature	**68.4**	**60.6**	**57**	**55**	**51.4**	**55.1**	**52.6**	**50**	**52.1**	**50**	**48.5**	随机森林
	54.3	49.8	47.2	46.1	44.6	44	43.3	42.8	42.7	43.2	42.8	决策树
	43.7	39.5	38.4	36.7	36.2	35.9	34	33.5	0.32	31.1	31	*k* 邻近
	45.8	43.8	43.8	43.2	43.1	42.8	42.5	42.2	41.8	41.1	41	逻辑回归
Pinlogger	**64.6**	**59.5**	**58.2**	**56.1**	**51.9**	**51.1**	**49.8**	**50.3**	**50.4**	**48.7**	**47.8**	随机森林
	53.1	48.9	47	45.6	44.6	44.5	43.5	43.4	43.3	43	42.3	决策树
	40.2	39.4	39.2	39.1	39.1	39.2	39.1	39	39.1	39	38.6	*k* 邻近
	43.7	43.1	43	42.5	42.1	41.6	41.2	41	40.9	41	40.8	逻辑回归
Textlogger	**68**	**59.5**	**56.9**	**54.8**	**53.2**	**52.3**	**51**	**50.9**	**50.7**	**50.3**	**49.3**	随机森林
	58.1	53.5	50.8	47.5	45.6	43.5	42.8	40.8	39.3	37.6	36.5	决策树
	48.3	39.1	36.2	33.8	30.9	28	26.8	24.4	23.1	21.2	20.2	*k* 邻近
	75.1	**68.1**	**66.1**	**60.6**	**59.8**	**55.3**	**55**	**55**	**52.7**	**51.4**	**48.3**	逻辑回归
Tapprints	71.5	63.4	60	57.3	54.5	52	50.9	49.4	46.8	45.2	44.4	随机森林
	59.1	53.5	50.5	48.2	45.4	44.4	42.6	41.6	40	38.1	37	决策树
	55.4	53.1	51.8	50.1	48.2	45.6	46.3	43.3	42	41.1	38.3	*k* 邻近
	71.8	**65.2**	**63.3**	**59.9**	**55.1**	**53.7**	**53.1**	**51.3**	**50.4**	**49.9**	**48**	逻辑回归
Taplogger	26.9	24.1	23.9	21.3	19.6	19	19.3	17.6	17.2	17.1	15.5	随机森林
	23.4	22.5	19.5	18	16.7	16.4	16	14.9	15.1	14.3	13.6	决策树
	29.5	27.5	23.7	21.4	19.3	19.5	18.9	17.1	16.5	16.2	14.1	*k* 邻近
	32.6	**32.4**	**33.2**	**28.6**	**25.2**	**24.9**	**25.2**	**24.9**	**23.8**	**23.5**	**19.1**	逻辑回归
Input-extraction	**64.6**	**55.8**	**53.5**	**54.9**	**50.4**	**48.4**	**51.3**	**48.7**	**50.4**	**48.7**	**49.6**	随机森林
	47.9	47.1	46.2	44.7	43.6	42.4	42.2	42	41.8	40.9	40.9	决策树
	59.2	48.8	48.7	48.1	47.8	46.8	46.1	45.7	45.2	45.1	44.9	*k* 邻近
	61.1	55.3	52.7	50.2	48.3	46.8	46.5	45.9	44.6	44.7	44.5	逻辑回归
Practicality	**94.5**	**94**	**91.5**	**90.3**	**90.8**	**86**	**85**	**85**	**84.6**	**82.3**	**80.5**	随机森林
	92	90.2	89.5	89.2	87.9	87.7	86.1	84.7	83	82.1	81.4	决策树
	43.9	39	37.1	33.8	29.5	29.1	28.8	28	27.4	26.5	25.4	*k* 邻近
	19.7	19.6	19.2	19.1	18.1	17.4	16.1	16.1	17.2	14.7	15.5	逻辑回归

由表 6 中的实验结果可看出,由于噪声的注入降低了各点击位置对应特征之间的区分度,所以在任意模型下,通过对传感器读数进行平移混淆均能够有效地降低所有 8 种输入侧信道的攻击准确率.随着混淆程度的增大,防御效果越发明显,各侧信道最优模型下混淆程度ε=1 时,准确率平均下降约 1 个~9 个百分点;当混淆程度增加至ε=10 后,预测准确率平均下降约 13 个~27 个百分点.此外,侧信道的初始预测准确率越高,信号混淆导致的准确率下降幅度越明显.

输入侧信道的单次点击预测误差会随着预测序列长度的增加而累积,以攻击效果最优的 Textlogger 侧信道为例,攻击长度为 4 的 PIN 时,未进行信号混淆情况下,侧信道的平均成功率约为 32%,即有约 9 成的概率在 6 次尝试之内攻破 PIN.进行了混淆程度为ε=1 的平移混淆后,Textlogger 攻击 PIN 的平均成功率为 21.5%,达到相同的破解概率需要 10 次尝试.当混淆因子增加到 10 后,尝试次数至少需要 45 次,但是大多数智能设备在自动锁屏前仅允许 5~10 次失败,因此,由平移混淆实现的侧信道防御方案能够有效抑制输入侧信道攻击.

5.2 追踪侧信道防御验证

虽然追踪侧信道的相关研究在运动传感器侧信道领域的比重较小,但是由于追踪侧信道实施的前提假设更少,且不同类型设备的传感器硬件误差存在明显差异,追踪侧信道的威胁同样不容忽视.本节中,我们对表 3 中的 3 种追踪侧信道进行实际攻防实验.将表 1 中的 10 台设备正面朝上水平放置,以 5s~7s 内的加速度传感器、陀螺仪和方向传感器信号做为独立初始样本,识别对应设备.

与输入侧信道实验一致,为验证数据集的可用性以及数据集对于学习模型的影响,首先使用多种机器学习模型实现上述追踪侧信道攻击.通过不同学习模型实现的追踪侧信道在原始数据下的攻击结果见表 7.

Table 7 Impact of learning model on experimental tracking side channels (%)

表 7 实验环境下学习模型对于追踪侧信道的影响 (%)

追踪侧信道	学习模型					
	SVM	决策树	随机森林	*k* 邻近	贝叶斯	逻辑回归
MobileTracking	10.8	**98.2**	96.4	85.2	11.5	20.2
TrackingExploring	12.3	98.4	**99.3**	85.8	12.5	17.2
AccelPrint	9.9	97.9	**98.8**	66.4	11.5	12.6

表 7 中的结果表明:在本文数据集中,随机森林模型更适合构建 TrackingExploring 侧信道与 AccelPrint 侧信道,决策树模型更适合于构建 MobileTracking 侧信道.下一步,通过平移混淆对传感器数据添加随机噪声,混淆因子$\varepsilon\in\{0,1,2,3,4,5,6,7,8,9\}$,分别使用随机森林、决策树和 *k*-NN 模型构建 3 种追踪侧信道,实验结果见表 8.

Table 8 Results of defense experiment against tracking side channels (%)

表 8 追踪侧信道对抗实验结果 (%)

追踪侧信道	ε										
	0	1	2	3	4	5	6	7	8	9	学习模型
MobileTracking	96.4	91.8	92	91.7	91.4	91.7	91.6	90.7	90.3	91	随机森林
	98.2	**88.1**	**87.9**	**87.8**	**87**	**87.6**	**87.5**	**87.1**	**87**	**87.8**	决策树
	85.2	86.6	87.2	86.2	86.7	86	86.4	86.4	86.2	86.9	*k* 邻近
TrackingExploring	**99.3**	**92.9**	**92.6**	**92.4**	**92.1**	**92.6**	**92.3**	**92.6**	**92.1**	**92.1**	随机森林
	98.4	86.9	86.2	85.9	86.2	85.7	85	84.4	84.9	84.4	决策树
	85.8	86.8	86.5	86.7	86.3	86.9	86.3	86.4	85.5	84.3	*k* 邻近
AccelPrint	**98.8**	**76.3**	**76.2**	**76.1**	**77.2**	**77.2**	**76.7**	**77.7**	**76.4**	**76.4**	随机森林
	97.9	74.6	74.9	75.6	76.1	75.8	75.6	76.6	75.6	76.1	决策树
	66.4	64.2	64.3	64.1	65.5	66.9	63.7	61.6	62.8	61.8	*k* 邻近

根据表 8 中的实验结果,信号混淆对于追踪侧信道的干扰主要呈现于两个方面.

- 首先,防御机制应对不同学习模型时存在差异,信号混淆能够显著抑制基于决策树和随机森林模型构建的追踪侧信道攻击的准确率,但在对抗由 *k*-NN 模型构建的追踪侧信道时反而产生反作用.该现象与第 4.2.2 节中的分析结果一致,构建侧信道所提取的特征当中存在数值较大且区分度低,但不易受噪声影响的属性,因此进行噪声注入后反而导致攻击准确率上升.然而,该情况并不会阻碍实际防御效果,因为侧信道预处理过程中的归一化能够消除值域的干扰,即使未进行归一化处理,提升后的攻击准确率仍然远低于其他模型下构建的侧信道.
- 其次,混淆程度对于追踪侧信道防御效果的影响无关,虽然噪声注入能够立刻较大程度地抑制攻击准确率,但是增加混淆程度并不能明显增强对于追踪侧信道的防御效果,其原因在于设备之间硬件差异较大,导致对应样本类别间的边界比较清晰.

上述结果有利于决定实际防御过程中的传感器信号混淆程度范围,仅需考虑合法应用中传感器相关功能对于噪声的承受能力.

下一步讨论待识别设备数量对侧信道防御的影响情况.我们从表 1 中随机筛选 5 台设备样本进行攻击实验,实验中的追踪侧信道均由最优模型构建,实验结果见表 9.

Table 9 Impact of number of device on defense against tracking side channels (%)

表 9 追踪侧信道对抗效果受设备数量影响情况 (%)

追踪侧信道	ε										
	0	1	2	3	4	5	6	7	8	9	学习模型
MobileTracking	99.1	92.3	92.2	92.2	91.5	91.4	91.3	91.3	91.2	90.6	决策树
TrackingExploring	99.9	95.5	95.5	95.1	95.2	95	94.8	94.5	94.3	94	随机森林
AccelPrint	99.5	98	98	97.8	97.8	97.6	97.7	97.6	97.5	97.4	随机森林

比较表 8 与表 9 中的实验结果,信号混淆方案的防御效果与设备数量成正比例关系,追踪侧信道待识别的设备数量越多,则防御效果越好.实际的攻击场景中,待识别的设备数量可能远远多于 10 台,因而基于信号混淆的侧信道防御机制能够在实际应用中产生更加优异的对抗效果.

本节中,我们从应用方面验证了本文所提出的运动传感器侧信道防御方案能够有效干扰各种类型侧信道攻击,通过注入少量噪声,即能够在不影响用户体验的前提下实现无差别的运动传感器侧信道防御.该方案与侧信道类型、侧信道构建模型和特征无关,具有非常良好的普适性与防御能力.

6 相关工作

6.1 运动传感器侧信道

6.1.1 输入侧信道

运动传感器被广泛应用于构建侧信道攻击,攻击者通过学习传感器数据与点击行为之间的映射关系,推测用户的输入信息[2,3].加速度传感器、方向传感器、陀螺仪等运动传感器都可以作为侧信道媒介[39].Cai 等人[40]利用陀螺仪和方向传感器构建了 TouchLogger 侧信道攻击,首次指出按键产生的设备震动与键位之间存在高相关性,该理论成为了输入侧信道的最重要理论之一.TapLogger[30]侧信道由陀螺仪和加速度传感器实现,作者提出,通过加速度信号的波形区分点击事件的发生.文献[28]通过合理的特征处理,利用加速度传感器与陀螺仪实现了对长序列文本输入的有效攻击.Noor 等人[41]的研究指出,相邻点击事件之间的手势改变同样能够用于推测点击位置;Negulescu 等人[42]在此基础上实现了侧信道的构建.除了 Android 系统,Marquardt 等人[43]在 iOS 下实现了输入侧信道,作者通过放置在键盘附近的 iPhone 收集用户敲击键盘时产生的桌面震动信息,推测点击行为.某些智能穿戴设备同样能够被用于构建运动传感器侧信道攻击[14].

上述输入侧信道的实际攻击目标均为用户点击触屏的位置,因此在攻击连续的输入序列时会产生累计误差.Aviv 等人[32]将侧信道的攻击对象改变为完整的输入序列,通过拟合用户输入完整 PIN 时产生的加速度信号,提取统计特征,识别特定的输入序列.这类输入侧信道与基于行为特征的身份认证[44,45]方法非常相似.除字符密码外,攻击也适用于图形密码[46,47].然而,仅 4 位长度的 PIN 就存在 10^4 种排列组合,如何构建完整可靠的训练集,是这类输入侧信道有待解决的首要问题.

6.1.2 追踪侧信道

追踪侧信道通过传感器的硬件误差,提取指纹信息作为识别设备的唯一标识.Bojinov 等人[38]通过提取加速度传感器线性误差关系中的增益误差与偏移误差,构建了追踪侧信道攻击.当用户使用移动设备访问网站时,攻击者可以在服务器端通过浏览器获得加速度信息用于识别匿名用户.除此之外,该研究还指出,麦克风等非运动传感器同样能够帮助进行用户识别.Das 等人[6]同样通过 Web 浏览器获取加速度传感器读数,构建侧信道进行用户追踪.不同的是,该侧信道并没有直接使用增益误差和偏移误差作为设备特征,而是提取其他统计特征用来反映传感器的硬件标识.研究者分析了在实际的攻击场景下追踪侧信道的表现情况[7],为提高侧信道攻击准确率,作者们新增了线性加速度传感器和陀螺仪,并实施更合理的特征工程方案.Dey 等人[8]利用移动设备加速度传感器的独有特征构建追踪侧信道,在实验环境和实际环境中均取得非常优异的表现.

6.2 传感器侧信道防御

针对移动设备键盘恶意按键推理攻击的可行性已经被多个研究工作所证实,但是在保护方面研究较少.对

传感器进行访问控制是一种可行的侧信道防御方案.Conti 等人[16]提出了一种基于上下文的访问控制机制,该机制可以将用户从人工设置访问权限中释放出来,但是他们所实现的机制需要对已有的操作系统进行复杂的修改,而本文提出的方法只需要在框架层中嵌入少量程序.此外,限制访问控制机制实际应用的最大问题在于无法防御来自具有合法权限的 APP 所进行的侧信道攻击,相比之下,本文方法对应用层程序实现无差别防御.文献[14]和文献[15]提出,通过强制降低传感器采样频率或禁止传感器运行的方式防御传感器侧信道攻击.然而,这种行为对于非恶意应用的影响非常严重,许多 APP,例如射击游戏等,需要较高的采样频率以达到用户满意的运行效果.我们的防御方案能够在进行有效防御的同时,保证合法应用的正常运行.

Shrestha 等人[18]在用户输入敏感信息的过程中向传感器读数中注入强烈噪声的方式完全破坏传感器读数,然而该方案不但可能造成正常应用程序的失效,还可能由于突破 Android 的沙盒机制而被判定为恶意行为.此外,该方案容易被攻击者利用注入有利于构建侧信道的信息[23,24].由于无法准确判断用户何时进行敏感信息输入,该方案仍然依赖于安全意识普遍较低的用户决策.与之相比,我们的防御过程实施于系统框架层,不会被恶意攻击者绕过或利用,此外,由于完全透明于应用,防御将不会有用户行为的干扰.

输入侧信道的基本假设是攻击者知道目标用户使用的键盘尺寸和布局,Young 等人[17]首次提出随机改变目标键盘的布局是针对输入侧信道攻击的有效保护策略.在此基础上,Maiti 等人[48]对默认布局中的按键大小、排序等采取不同程度随机化,一定程度上平衡了随机键盘策略的易用性和安全性.通过改变键盘布局的防御方法具有明显的局限性:首先,改变广泛使用且用户已经非常熟悉的默认键盘对于绝大部分用户而言是不友好的,而且除了系统的默认键盘外,很多 APP(微信,支付宝等)自带键盘,难以将键盘布局随机化策略应用到所有 APP 中;其次,布局随机化策略无法防御同样利用运动传感器的追踪侧信道攻击.

已有的工作在以下两个方面存在缺陷:首先,已有研究无法有效平衡用户体验与防御能力,要么牺牲用户体验来提高防御效果,要么保证了用户体验而防御能力较差;其次,已有的研究无法做到对各种类型侧信道的普适防御.本文提出的防御方法有效地解决了上述问题:通过在系统框架层进行信号混淆,能够对各种类型侧信道的构建过程进行干扰,实现了该防御方案的有效性和灵活性.此外,我们在先前的工作[21]中分析了合法应用程序与侧信道对于传感器数据精度的差异,讨论了各种类型运动传感器相关功能的噪声承受上界,提出了各类合法功能的建议混淆范围,进而保证防御方法的可用性.与其他研究相比,该防御方案实现了防御能力与用户体验的平衡,具有优异的应用价值.

7 总 结

本文针对移动设备运动传感器侧信道攻击,提出了基于 Laplace 机制的传感器信号混淆防御方案,并对防御原理进行了详细和全面的理论分析.本文的防御方案中,通过平移混淆方式向传感器读数中无差别地注入服从 Laplace 分布的少量随机噪声,在保证 APP 正常运行的前提下,有效降低各种类型的运动传感器侧信道攻击成功率.该防御方案部署在系统框架层,对于攻击者和用户完全透明,不会破坏系统原有安全机制,具有良好的可用性、普适性和灵活性.首先,对运动传感器侧信道的构建过程进行了分析,讨论运动传感器侧信道通用模型;然后,从理论层面分析了信号混淆干扰运动传感器侧信道学习阶段的原理,进而证明本文提出的信号混淆方案对于符合模型的传感器侧信道均有效;最后,对 8 种典型的输入侧信道以及 3 种追踪侧信道进行防御测试,验证防御方案在应对实际攻击时的有效性,其中,混淆程度ε=10 时,平移混淆降低输入侧信道单次预测准确率平均约 19 个百分点,降低追踪侧信道单次设备识别准确率平均约 13 个百分点.本文的研究不仅能够在侧信道防御的实际应用中发挥积极作用,对后续运动传感器侧信道相关工作也具有重要的参考价值.

References:

[1] Spreitzer R, Moonsamy V, Korak T, Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices. IEEE Communications Surveys & Tutorials, 2018,20(1):465−488. [doi: 10.1109/COMST.2017.2779824]

[2] Nahapetian A. Side-Channel attacks on mobile and wearable systems. In: Proc. of the Consumer Communications & Networking Conf. Piscataway: IEEE, 2016. 243−247. [doi: 10.1109/CCNC.2016.7444763]

[3] Cai L, Chen H. On the practicality of motion based keystroke inference attack. In: Katzenbeisser S, ed. Proc. of the 5th Int'l Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag, 2012. 273–290. [doi: 10.1007/978-3-642-30921-2_16]

[4] Lee YJ. Detection of movement and shake information using android sensor. Advanced Science and Technology Letters, 2015,90: 52–56. [doi: 10.14257/astl.2015.90.12]

[5] Shala U, Rodriguez A. Indoor positioning using sensor-fusion in android devices [MS. Thesis]. Kristianstad: Kristianstad University, 2011.

[6] Das A, Borisov N, Caesar M. Tracking mobile Web users through motion sensors: Attacks and defenses. In: Proc. of the Network and Distributed System Security Symp. Rosten: Internet Society, 2016. [doi: 10.14722/ndss.2016.23390]

[7] Das A, Borisov N, Chou E. Every move you make: Exploring practical issues in smartphone motion sensor fingerprinting and countermeasures. Proc. on Privacy Enhancing Technologies, 2018,2018(1):88–108. [doi: 10.1515/popets-2018-0005]

[8] Dey S, Roy N, Xu W, Choudhury RR, Nelakuditi S. AccelPrint: Imperfections of accelerometers make smartphones trackable. In: Proc. of the Network and Distributed System Security Symp. Rosten: Internet Society, 2014. [doi: 10.14722/ndss.2014.23059]

[9] Tang BX, Wang ZB, Wang R, Zhao L, Wang LN. Niffler: A context-aware and user-independent side-channel attack system for password inference. Wireless Communications and Mobile Computing, 2018,2018:Article ID 4627108. [doi: 10.1155/2018/4627108]

[10] Zhang W, He H, Zhang QZ, Kim T. PhoneProtector: Protecting user privacy on the android-based mobile platform. Int'l Journal of Distributed Sensor Networks, 2014,10(2):1–10. [doi: 10.1155/2014/282417]

[11] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Stealing pins via mobile sensors: Actual risk versus user perception. Int'l Journal of Information Security, 2018,17(3):291–313. [doi: 10.1007/s10207-017-0369-x]

[12] Mohamed M, Shrestha B, Saxena N. SMAshed: Sniffing and manipulating android sensor data for offensive purposes. IEEE Trans. on Information Forensics and Security, 2017,12(4):901–913. [doi: 10.1109/TIFS.2016.2620278]

[13] Cai L, Machiraju S, Chen H. Defending against sensor-sniffing attacks on mobile phones. In: Proc. of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds. New York: ACM Press, 2009. 31–36. [doi: 10.1145/1592606.1592614]

[14] Maiti A, Jadliwala M, He J, Bilogrevic I. (Smart) watch your taps: Side-channel keystroke inference attacks using smartwatches. In: Proc. of the ACM Int'l Symp. on Wearable Computers. New York: ACM Press, 2015. 27–30. [doi: 10.1145/2802083.2808397]

[15] Owusu E, Han J, Das S, Perrig A, Zhang J. ACCessory: Password inference using accelerometers on smartphones. In: Proc. of the 12th Workshop on Mobile Computing Systems & Applications. New York: ACM Press, 2012. 1–6. [doi: 10.1145/2162081.2162095]

[16] Conti M, Nguyen VTN, Crispo B. CRePE: Context-related policy enforcement for Android. In: Burmester M, ed. Proc. of the 13th Int'l Conf. on Information Security. Berlin: Springer-Verlag, 2010. 331–345.

[17] Ryu YS, Koh DH, Aday BL, Gutierrez XA, Platt JD. Usability evaluation of randomized keypad. Journal of Usability Studies, 2012, 5(2):65–75.

[18] Shrestha P, Mohamed M, Saxena N. Slogger: Smashing motion-based touchstroke logging with transparent system noise. In: Proc. of the 9th ACM Conf. on Security & Privacy in Wireless and Mobile Networks. New York: ACM Press, 2016. 67–77. [doi: 10.1145/2939918.2939924]

[19] Qing SH. Research progress on Android security. Ruan Jian Xue Bao/Journal of Software, 2016,27(1):45–71 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[20] Dwork C, Mcsherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. In: Halevi S, ed. Proc. of the Theory of Cryptography Conf. Berlin: Springer-Verlag, 2006. 265–284.

[21] Tang BX, Wang LN, Wang R, Zhao L, Wang DL. A defensive method against android physical sensor-based side-channel attack based on differential privacy. Joural of Computer Research and Development, 2018,55(7):1371–1392 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2018.20170982]

[22] Wang YJ, Wu JZ, Zeng HT, Ding LP, Liao XF. Covert channel research. Ruan Jian Xue Bao/Journal of Software, 2010,21(9): 2262–2288 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

[23] Laskov P, Lippmann R. Machine learning in adversarial environments. Machine Learning, 2010,81(2):115−119. [doi: 10.1007/s10994-010-5207-6]

[24] Auer P, Cesa-Bianchi N. On-Line learning with malicious noise and the closure algorithm. Annals of Mathematics & Artificial Intelligence, 1998,23(1-2):83−99.

[25] Malkin N, Harbach M, De Luca A, Egelman S. The anatomy of smartphone unlocking: Why and how Android users around the world lock their phones. GetMobile: Mobile Computing and Communications, 2016,20(3):42−46. [doi: 10.1145/3036699.3036712]

[26] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Touchsignatures: Identification of user touch actions and pins based on mobile sensor data via javascript. Journal of Information Security and Application, 2016,26:23−38. [doi: 10.1016/j.jisa.2015.11.007]

[27] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Stealing pins via mobile sensors: Actual risk versus user perception. Int'l Journal of Information Security, 2018,17(3):291−313. [doi: 10.1007/s10207-017-0369-x]

[28] Ping D, Sun X, Mao B. Textlogger: Inferring longer inputs on touch screen using motion sensors. In: Proc. of the 8th ACM Conf. on Security & Privacy in Wireless and Mobile Networks. New York: ACM Press, 2015. No.24. [doi: 10.1145/2766498.2766511]

[29] Miluzzo E, Varshavsky A, Balakrishnan S, Choudhury RR. Tapprints: Your finger taps have fingerprints. In: Proc. of the 10th Int'l Conf. on Mobile Systems, Applications, and Services. New York: ACM Press, 2012. 323−336. [doi: 10.1145/2307636.2307666]

[30] Xu Z, Bai K, Zhu SC. TapLogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In: Proc. of the 15th ACM Conf. on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2012. 113−124. [doi: 10.1145/2185448.2185465]

[31] Shen C, Pei SC, Yang ZY, Guan XH. Input extraction via motion sensor behavior analysis on smartphones. Computers & Security, 2015,53:143−155. [doi: 10.1016/j.cose.2015.06.013]

[32] Aviv AJ, Sapp B, Blaze M, Smith JM. Practicality of accelerometer side channels on smartphones. In: Proc. of the 28th Annual Computer Security Applications Conf. New York: ACM Press, 2012. 41−50. [doi: 10.1145/2420950.2420957]

[33] Zheng N, Bai K, Huang H, Wang H. You are how you touch: User verification on smartphones via tapping behaviors. In: Proc. of the IEEE 22nd Int'l Conf. on Network Protocols. Piscataway: IEEE, 2014. 221−232. [doi: 10.1109/ICNP.2014.43]

[34] Peng HC, Long FH, Ding C. Feature selection based on mutual information: Criteria of max-dependency, max-relevance, and min-redundancy. IEEE Trans. on Pattern Analysis & Machine Intelligence, 2005,27(8):1226−1238. [doi: 10.1109/TPAMI.2005.159]

[35] Liu XH, Li S. An optimized algorithm of decision tree. Ruan Jian Xue Bao/Journal of Software, 1998,9(10):797−800 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/9/797.htm

[36] Maaten L, Hinton G. Visualizing data using *t*-SNE. Journal of Machine Learning Research, 2008,9(2008):2579−2605.

[37] Maaten L. Accelerating *t*-SNE using tree-based algorithms. Journal of Machine Learning Research, 2014,15(1):3221−3245.

[38] Bojinov H, Boneh D, Michalevsky Y, Nakibly G. Mobile device identification via sensor fingerprinting. arXiv preprint arXiv: 1408.1416, 2014.

[39] Shen C, Yu T, Yuan S, Guan XH. Performance analysis of motion-sensor behavior for user authentication on smartphones. Sensors, 2016,16(3):345−365. [doi: 10.3390/s16030345]

[40] Cai L, Chen H. TouchLogger: Inferring keystrokes on touch screen from smartphone motion. In: Proc. of the 6th USENIX Workshop on HotSec. New York: ACM Press, 2011. 9−15.

[41] Noor MFM, Ramsay A, Hughes S, Ogers S, Williamson J, Smith RM. 28 frames later: Predicting screen touches from back-of-device grip changes. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. New York: ACM Press, 2014. 2005−2008. [doi: 10.1145/2556288.2557148]

[42] Negulescu M, Mcgrenere J. Grip change as an information side channel for mobile touch interaction. In: Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems. New York: ACM Press, 2015. 1519−1522. [doi: 10.1145/2702123.2702185]

[43] Marquardt P, Verma A, Carter H, Traynor P. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In: Proc. of the 18th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2011. 551−562. [doi: 10.1145/2046707.2046771]

[44] Luca AD, Hang A, Brudy F, Lindner C, Hussmann H. Touch me once and i know it's you! Implicit authentication based on touch screen patterns. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. New York: ACM Press, 2012. 987−996. [doi: 10.1145/2207676.2208544]

[45] Shahzad M, Liu AX, Samuel A. Behavior based human authentication on touch screen devices using gestures and signatures. IEEE Trans. on Mobile Computing, 2017,16(10):2726−2741. [doi: 10.1109/TMC.2016.2635643]

[46] Liu JY, Zhong L, Wickramasuriya J, Vasudevan V. uWave: Accelerometer-based personalized gesture recognition and its applications. Pervasive and Mobile Computing, 2009,5(6):657−675. [doi: 10.1016/j.pmcj.2009.07.007]

[47] Andriotis P, Tryfonas T, Oikonomou G, Yildiz C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proc. of the 6th ACM Conf. on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2013. 1−6. [doi: 10.1145/2462096.2462098]

[48] Maiti A, Crager K, Jadliwala M, He J, Kwiat K, Kamhoua C. Randompad: Usability of randomized mobile keypads for defeating inference attacks. In: Proc. of the IEEE Euro S&P Workshop on Innovations in Mobile Privacy & Security (IMPS). Piscataway: IEEE, 2016.

附中文参考文献:

[19] 卿斯汉.Android 安全研究进展.软件学报,2016,27(1):45−71. http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[21] 唐奔宵,王丽娜,汪润,赵磊,王丹磊.基于差分隐私的 Android 物理传感器侧信道防御方法.计算机研究与发展,2018,55(7):1371−1392. [doi: 10.7544/issn1000-1239.2018.20170982]

[22] 王永吉,吴敬征,曾海涛,丁丽萍,廖晓锋.隐蔽信道研究.软件学报,2010,21(9):2262−2288. http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

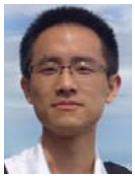
[35] 刘小虎,李生.决策树的优化算法.软件学报,1998,9(10):797−800. http://www.jos.org.cn/1000-9825/9/797.htm

唐奔宵(1991－),男,湖北黄石人,博士,CCF 学生会员,主要研究领域为 Android 隐私保护,机器学习.

赵磊(1985－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为系统安全,软件分析.

王丽娜(1964－),女,博士,教授,博士生导师,主要研究领域为系统安全,信息隐藏.

陈青松(1995－),男,学士,主要研究领域为移动隐私保护.



汪润(1991－),男,博士,主要研究领域为移动设备隐私保护,机器学习.