分类号_____ 编 号_____

U D C_____ 密 级_____

南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

本科生毕业设计（论文）

题　　目：跨设备的 Android 应用录制与回放工具

姓　　名：余添诚

学　　号：11712019

系　　别：计算机科学与工程系

专　　业：计算机科学与技术专业

指导教师：刘烨庞教授

2021 年　月　日

诚信承诺书

1. 本人郑重承诺所呈交的毕业设计（论文），是在导师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料均真实可靠。
2. 除文中已经注明引用的内容外，本论文不包含任何其他人或集体已经发表或撰写过的作品或成果。对本论文的研究作出重要贡献的个人和集体，均已在文中以明确的方式标明。
3. 本人承诺在毕业论文（设计）选题和研究内容过程中没有抄袭他人研究成果和伪造相关数据等行为。
4. 在毕业论文（设计）中对侵犯任何方面知识产权的行为，由本人承担相应的法律责任。

作者签名: _____

_____ 年___ 月___ 日

目　录

摘 要

随着移动设备的日趋流行，对于移动应用的自动化测试成为降低开发者时间成本和保障产品质量的关键点。本研究设计并实现了一套能够在不同的 Android 设备上录制和回放应用输入的工具，并提升录制与回放的性能及准确性等相关性能参数。在避免使用定制化系统或修改被测应用源代码的情况下，能够准确高效地录制来自触屏及各项传感器（如陀螺仪、GPS、摄像头）的输入，并在不同型号的 Android 设备上自适应地回放。我们通过实验展示了该工具在? 种不同的实验环境下（含不同型号真实设备以及模拟器）以及超过? 款商业闭源或开源应用上测试的结果。

关键词： Google Android, 应用测试, 移动应用, 录制与回放

ABSTRACT

With the increasing popularity of mobile devices, automated testing for mobile applications has become the key point for lowering developers' time costs and assuring product quality. The main goal of this work is to implement a Record-and-Replay system for various Android devices, improving the quality and accuracy of the results, without using customized operating system or modifying application source code, while be able to accurately and efficiently record from touch screen and various sensors (e.g. gyroscope, GPS, camera), and replay on different models of Android devices in an adaptive manner. We demonstrate the tool's ability by performing experiments on ? different environments (including various models of real-world devices and emulators) with over ? commercial closed-source or open-source applications.

Keywords: Google Android, App testing, Mobile applications, Record-and-replay

第一章 导言

随着移动设备的日趋流行，自动化测试移动应用的关键性日渐显著。然而，在目前的企业开发环境中，应用测试仍然主要以高时间成本的人工方式进行，能够在不同设备上进行录制和回放将显著地减轻开发者和测试人员的负担。

与传统程序不同的是，移动应用中多样化的用户输入方式——触摸屏和不同的传感器（如陀螺仪，GPS，摄像头），以及屏幕尺寸和系统版本的差异化，给应用的自动化测试带来了挑战。触屏、传感器、网络，乃至于随机数生成器等难以通过传统方法录制和重放的因素对于移动应用的用户界面交互结果至关重要。移动设备较弱的性能也使精确地录制与回放对时间敏感的序列存在困难。

现今学术界与工业界已有多种不同录制与回放的方案，但各自均有一定的缺陷和局限性。基于定制系统的方案 [1] 需要针对每个机型编写和安装定制化系统，开发以及维护成本高昂；基于内核事件的方案 [2] 从内核级别获取的传感器数据有限，难以满足录制较高层级数据（网络、GPS）的需求；基于静态插桩 [3] 则难以对加密的商业闭源应用使用，不便于商业公司外派测试工作；基于屏幕坐标的回放 [2] 需要在不同的设备上多次重复录制相似的输入，增加用户的时间成本；基于 root 权限的动态插桩 [2] 在部分品牌或机型上难以实现，并可能导致机器失去品牌保修。

文献 [4] 通过实证研究指出，现有的录制与回放工具在有效性、性能以及可靠性上仍然无法满足开发者的实际需求。在研究中，来自微信 [5] 的开发者提出其理想的录制与回放工具所应满足的功能与限制。在文中，微信开发者希望存在相关工具能够：（一）开源具体实现；（二）基于坐标录制动作；（三）基于界面组件录制操作；（四）对应用具体状态不敏感；（五）记录多个操作之间的时间间隔；以及尽量避免：（一）需要对应用插桩；（二）需要定制化系统；（三）需要 root 权限；（四）需要应用源代码。

本文提出一种跨平台、跨设备的 Android 应用录制与回放工具，通过静态修改应用文件载入插桩类库，在运行时动态插桩应用以及系统关键库调用，在最大程度地规避上述局限性的情况下高效地提供可自适应环境、状态无关、时间准确、对多种输入有效的录制与回放。通过一定策略对关键目标函数的插桩，该工具得以在无需用户人工介入进行应用或平台相关的配置的条件下，自动记录各类不同输入的内容和上下文数据。录制用户的 UI 操作时，该工具对 Android 系统库内处理用户操作的函数进行插桩，截取具体输入以及目标界面组件的信息，从而实现不受屏幕坐标影响、对界面组件敏感的录制与回放功能；录制移动设备传感器数据时，该工具对应用内的传感器监听器进行插桩，在应用每次读取传感器数据时录制或回放传感器数据；录制网络、随机数等 Java 语言库功能时，该工具对语言库内关键调用进行插桩，使录制与回放过程不受外界或随机因素干扰，以保证录制与回放结果的确定性。

第二章 研究背景

本章节主要介绍本文所涉及的 Android 系统及应用的相关背景概念，如 Android 应用所能处理的不同类型用户输入，以及实现本文所述工具原型中使用到的技术背景。

2.1 Android 应用

Android 应用主要由 Java 编写，通过 Android SDK 编译为 Dalvik 字节码后由 Android Runtime (ART) 执行，部分代码亦可使用编译型语言编译为原生代码后加载执行。

在 Android 系统中，每个应用运行在自己独立的 ART 运行时里，通过 Android Framework 的 Java 库以及其他原生库（例如加解密相关的 libcrypto.so 和 libssl.so）提供应用所需的功能。

2.2 Android 应用界面

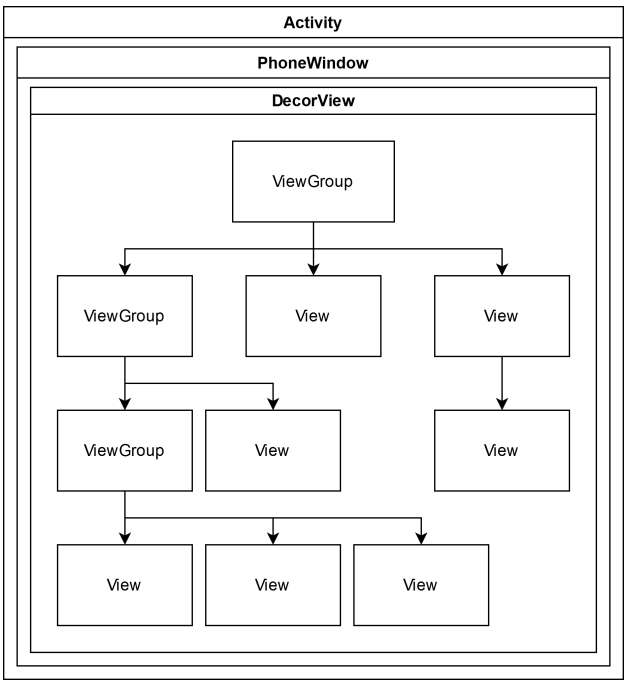

图 2.1: Android View 界面结构

Android Framework 为开发者提供了一系列预定义好的界面控件，例如文本框、选择框、按钮、图片和列表，开发者也可以继承 View 类开发自定义的控件，或继承 ViewGroup 类实现组合控件。每个 View 代表用户界面上的一个对象，应用运行时显示的界面实际为一个由 View 和 ViewGroup 组成的树状结构（见图 2.1）。应用可以在编译前通过资源文件定义界面结构，亦可在运行时动态地修改界面结构。

2.3 Android 用户输入

Android 应用中直接输入来源包含触摸屏和按键。用户对触摸屏的输入会触发 MotionEvent，通过 MotionEvent 的序列可以表达所有触摸屏操作（点击、滑动、长按）；按键输入会触发 KeyEvent。在用户触发事件后，Android 会从当前 Activity 的根节点向下搜索对应的 View 传递事件，路径中的 ViewGroup 可以选择自行处理或是继续传递给 View 子节点。应用亦可通过 Android SDK 以及 Java 核心库从硬件传感器、网络或其他来源获得输入。

2.4 动态插桩 ART VM 代码

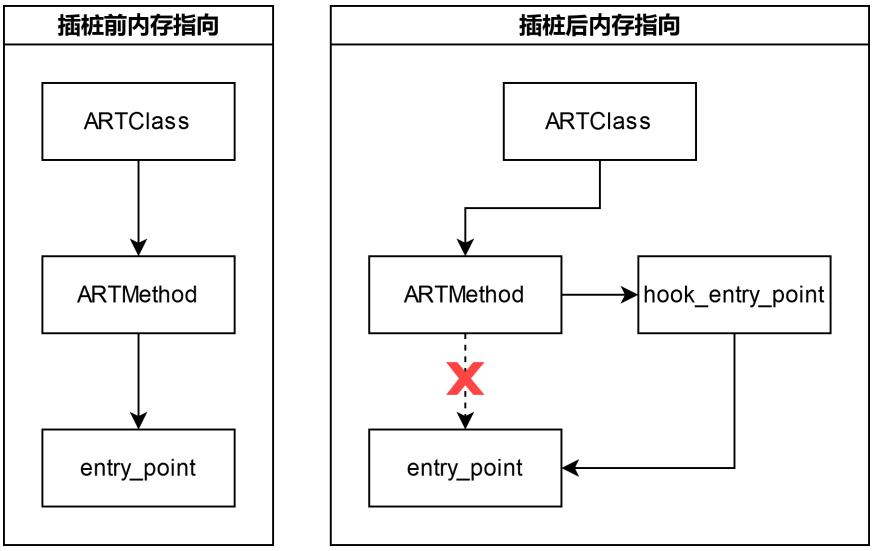

图 2.2: 动态插桩 ART 方法实现

在 ART 中，每个 Java Class 都由内存中的一个 ARTClass 对象代理内部数据结构，其中每一个函数对应着一个 ARTMethod 结构体。ARTMethod 实例中储存着具体方法实现的类型以及调用入口，因此可以通过注入 ARTMethod 类的内部变量，达到修改对应类或原生函数具体实现的目的（见图 2.2）。在本文所述工具中，我们通过 Frida[6] 注入 ART 修改目的函数的地址，以劫持或修改函数输入输出结果。

第三章　架构设计和实现

本章节主要描述本工具的设计思想和原因，以及如何在有限的条件下实现满足工业界需求的功能。

3.1　设计总览

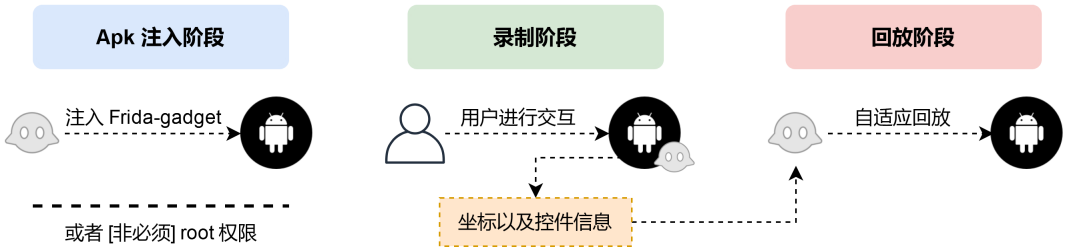

图 3.1: 设计总览

本工具主要由三个组件构成（见图 3.1）：Apk 注入器，录制代理以及回放代理。在开始录制前，先将动态插桩所需要的基础库注入到应用安装包中，如在 root 环境中可以跳过此步骤。在录制中，录制代理将会记录用户交互的坐标和控件信息，以及来自其他传感器（如 GPS、陀螺仪等）的相关数据。在回放时，回放代理将参考录制与回放所在设备的分辨率和尺寸差距，通过坐标和控件信息找到对应控件，并注入模拟的用户操作。

3.2　静态注入插桩模块

为了实现动态插桩，Frida 可以由 root 权限运行，或是借由注入到应用中的 Frida-gadget 模块进行操作。在本工具中，我们提供一个 Apk 注入器，自动将所需模块注入到应用原生库依赖中，以实现在应用启动时自动加载录制或回放代理。通过无需修改应用 Delvik 字节码的注入方式，本工具可以应用在经过字节码加密程序打包过的应用上。

3.3　动态插桩录制与回放

在录制与回放阶段，代理将录制或回放来自各种来源的输入数据。对于 Android 应用而言，主要的输入来源可以分为触屏/按键以及传感器。本工具通过注入一系列的 Android Framework API 函数以在框架层截获足够的上下文信息，而不失去对不同应用的泛用性。在下文中，我们将详细描述如何实现对不同输入来源的录制与回放。

表 3.1: 录制与回放触屏/按键时 Android Framework 的主要注入点

注入类	录制注入函数	回放注入函数
View	View(), setOnTouchListener(), dispatchKeyEvent()	draw(), dispatchDraw()
ViewGroup	dispatchKeyEvent()	-

3.3.1 触屏/按键的录制与回放

表 3.1中为本工具录制与回放触屏/按键操作时的主要注入点。在录制阶段中，以往的录制与回放工具 [7] 需要读取应用中的所有的 Activity 或 View 的子类并依次进行插桩，效率较低并且容易遗漏动态加载的类；本工具通过对 View 的构造器进行插桩，可以获得所有子类构造得到的对象实例并通过 setOnTouchListener() 监听控件所接收到的输入事件。在回放阶段中，回放代理插桩 View.draw() 和 View.dispatchDraw()，在控件绘制时更新控件签名并保留对控件的引用，允许在无需坐标，乃至于控件在屏幕上不可见的情况下对控件注入根据设备区别动态生成的输入事件。

3.3.2 传感器的录制与回放

表 3.2: 录制与回放传感器时 Android Framework 的主要注入点

注入类	注入函数
SensorManager	registerListener()
SensorEventListener (and subclasses)	onSensorChanged()
LocationListener	getLastKnownLocation(), requestLocationUpdates()
LocationListener (and subclasses)	onLocationChanged()

表 3.2中为本工具录制与回放传感器数据时的主要注入点。本工具对传感器的主动读取的函数以及被动事件驱动的监听器进行插桩，从而获得数据的接收类以及所接收的数据等回放时必须的上下文信息，并在回放时根据录制时的时间顺序将传感器数据注入对应类中。

参考文献

[1] HU Y, AZIM T, NEAMTIU I. Versatile yet Lightweight Record-and-Replay for Android[J/OL]. SIGPLAN Not., 2015, 50(10): 349–366. https://doi.org/10.1145/2858965.2814320.

[2] GOMEZ L, NEAMTIU I, AZIM T, et al. RERAN: Timing- and Touch-Sensitive Record and Replay for Android[C] // ICSE '13: Proceedings of the 2013 International Conference on Software Engineering. [S.l.]: IEEE Press, 2013: 72–81.

[3] Sahin O, Aliyeva A, Mathavan H, et al. RANDR: Record and Replay for Android Applications via Targeted Runtime Instrumentation[C/OL] // 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). 2019: 128 – 138. http://dx.doi.org/10.1109/ASE.2019.00022.

[4] LAM W, WU Z, LI D, et al. Record and Replay for Android: Are We There yet in Industrial Cases?[C/OL] // ESEC/FSE 2017: Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering. New York, NY, USA: Association for Computing Machinery, 2017: 854–859. https://doi.org/10.1145/3106237.3117769.

[5] TENCENT. WeChat[EB/OL]. 2021. https://www.wechat.com.

[6] Frida[EB/OL]. 2021. https://frida.re.

[7] GUO J, LI S, LOU J-G, et al. Sara: Self-Replay Augmented Record and Replay for Android in Industrial Cases[C/OL] // ISSTA 2019: Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis. New York, NY, USA: Association for Computing Machinery, 2019: 90–100. https://doi.org/10.1145/3293882.3330557.