计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(11):17−26 [doi: 10.15888/j.cnki.csa.006609]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于行为声明的可信性测试方法与可信度计算研究①

于学军, 肖　然

(北京工业大学 信息学部, 北京 100124)
通讯作者: 肖　然, E-mail: xran1003@163.com

摘　要: 针对软件行为的可信性进行了测试方法与度量标准的研究. 在测试方法上, 通过在软件开发阶段植入可信埋点模块的方式获取行为的动作路径, 以“言行一致”思想为依据, 将软件的行为声明与动作路径做比对, 得到可信性测试的新方法. 在判定标准上针对动作路径提出显性可信性判断指标和隐性可信指标, 在度量上提出基于 K-means 聚类的隐性指标判定模型, 并将此应用在单一行为的可信度计算以及相似行为的可信甄别上. 通过实验验证了方法的可行性, 为可信性测试提供了新的思路.

关键词: 软件可信性; 软件行为; 行为声明; 可信性测试; 可信度计算

引用格式: 于学军,肖然.基于行为声明的可信性测试方法与可信度计算研究.计算机系统应用,2018,27(11):17–26. http://www.c-s-a.org.cn/1003-3254/6609.html

Credibility Verification Method and Calculation Based on Application Behavior Declaration

YU Xue-Jun, XIAO Ran

(Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China)

Abstract: Based on Application Behavior Declaration (ABD), we proposed a new method for credibility calculation. It is based on the idea of “words and deeds”. In the software development phase, tracking module is implanted to extract the action path of the behavior. Then, we compare the behavior declaration of the software with the action path to achieve the purpose of evaluating whether the behavior is credible. Explicit and implicit indicators are proposed for judgment, as well as an implicit indicators model based on K-means clustering. This model is applied to the credible calculation of single behavior and the credible discrimination of similar behaviors. Experiments prove that this solution is feasible for providing new ideas for credibility testing.

Key words: software credibility; software behavior; behavior declaration; credibility verification; credibility calculation

基于网络的信息系统处在一个动态的开放环境中, 人们可以通过网络在任何时间任何地点进行信息的交互, 这比传统的信息系统在计算能力上有了显著的提升, 但与此同时, 信息系统的可信性问题也成为当今互联网时代面临的重大挑战[1–3].

本研究基于判定软件行为可信的“言行一致”的思想. 所谓“言行一致”思想指: “言”是指软件的预期行为, “行”是指软件的实际行为, “一致”指的是验证系统“言”与“行”的一致性. “言行一致”思想体现了行为与预期的关系, 符合目前学界对可信的定义[4]. 这也是上文所提出的本文依赖的可信标准.

行为声明是指应用软件针对自身行为进行描述的集合. 在该集合中, 行为包括软件的所有功能性行为、可能侵犯用户自身权利的行为、可能影响应用软件正常运行的行为和可能引发无法预期的软硬件环境配置改变的行为[4].

① 基金项目: 国家重点研发计划 (2017YFF0211801)
Foundation item: National Key Research and Development Plan of China (2017YFF0211801)
收稿时间: 2018-04-01; 修改时间: 2018-04-24; 采用时间: 2018-04-27; csa 在线出版时间: 2018-09-30

本篇论文的重点在于两个方面, 第一是探究适用于通用环境下的的基于行为声明可信性测试方法. 在基于行为声明的测试方法中, 本人提出了在软件全生命周期下运用行为声明保障软件可信性的模型[4], 得出了行为声明在软件开发过程中各个阶段的作用. 吕海庚提出在全生命周期可信过程保障模型的支撑下的 Web 应用软件的可信属性. 在此基础上, 提出了 Web 应用软件可信性验证模型, 并在此验证模型的支撑下, 提出了软件可信性测试方法[5]. 车乐林在针对行为声明的可信测试研究中, 基于移动端软件的特点提出可信行为声明的通用结构, 将研究得出的可信行为声明融入到应用的测试过程中, 得出了基于可信行为声明的移动应用测试模型和测试流程[6]. 刘妙晨以可信行为声明的内容结构和 REST 应用软件的结构特征及可信特征为基础, 提出基于行为声明的 REST 风格 Web 应用可信性测试方法[7]. 在这些研究中, 都是侧重于针对各软件环境下的特点对行为声明进行定义之后提出测试标准模型. 在基于行为声明的测试方法中, 还未有对如获取软件运行的实际行为, 如何感知到软件行为的动作路径的研究, 本文将侧重于此. 动作路径在本文是指：软件发生行为时执行的一系列程序设定的集合.

第二个研究重点是提出可信度的计算方法, 可信度在本文是指：软件实际行为与行为声明中行为的相似度. 在可信度量方面, 已有众多学者提出自己的方法. 韩冬冬等人提出了采用静态 hash 度量值, 动态行为特征值作为评判标准的的应用软件可信性混合度量的设计方法[8]. 熊刚等人提出采用多属性决策建模方法, 设计了一种策略来建立可信指标树, 这种方法是在按需驱动的基础上, 采用动态的方法来完成. 并为了减少主管权重计算的不确定性利用了模糊层次分析法, 为了提高赋权操作的公平性采用主客观权重相结合的方式. 在可信评价阶段, 他们主要采用了指标数据效用转换方法. 可信属性向量构造和向量减的相对近似度计算[9]. 赵玉洁等人运用因子分析法构建了针对 Web 软件的可信性评价指标体系. 在可信指标的权重计算上运用结构熵值法. 为构造专家评价信息的模糊评价矩阵运用了改进的证据合成方法. 在软件可信性等级评价上运用了置信度识别准则[10]. 綦磊升等人提出了基于模糊层次分析法的可信评估方法, 即将层次分析法和模糊综合评判法相结合, 克服了传统层次分析法中人作为个体的主观判断会对结果有很大影响的缺点, 使评估更加趋于合理[11]. 在以上研究中, 选取行为特征值, 专家评判和层次模糊分析法等的运用都侧重于软件行为的表现, 提出相应的可信指标加以判断, 存在一定的主观性. 本文将侧重于软件行为的发生过程, 针对软件行为发生时的事件类型以及运行参数, 运用 K-means 聚类方法提出一种分析模型, 结合行为声明对软件行为是否可信进行判定. 以及运用模型甄别相似行为是否可信.

1 测试方法的设计

本方法依据“言行一致”为判断标准[12], 通过将监控到的软件实际行为与行为声明作比较, 判断行为是否可信. 方法的关键在于对软件实际行为的监控, 以及可信度的计算.

1.1 制定行为声明

行为声明由一系列软件行为构成, 那么在本节将阐述本文对软件行为的表示方法. 本实验采用 JSON 对软件行为进行表示, 易于人阅读和编写. 软件行为可以看做完成一系列程序设定的过程. 本方法中将程序设定分为三种类型事件, 如图 1 所示, 根据是否可交互划分为点击事件与其他事件, 在其他事件中再根据是否可见将事件划分成可见的曝光事件与不可见的环境事件.

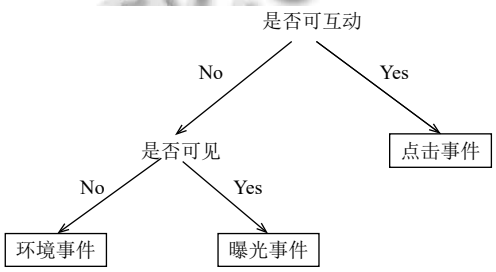


图 1 事件划分

点击事件表示当软件应用展现给用户的 UI 元素可点击且点击之后有反馈动作时触发, 比如一个按钮被点击会触发点击埋点上报按钮的点击事件. 数据格式会携带触发参数, 预期关联事件信息等.

曝光事件表示软件应用展示给用户的 UI 元素出现在界面上时触发, 比如一个图片展示给用户时会触发曝光埋点上爆图片的曝光事件. 数据格式会携带一组曝光参数.

环境事件表示软件应用发生不可见的动作时会触发, 比如调用系统的喇叭来播放音乐会触发环境埋点的声卡环境事件. 数据格式会携带当前事件发生时的系统参数, 比如内存使用率, 网络数据包等等.

一个“行为”即行为声明, 则是由以上三种类型的事件组成. 可用如图 2 中的结构表示.

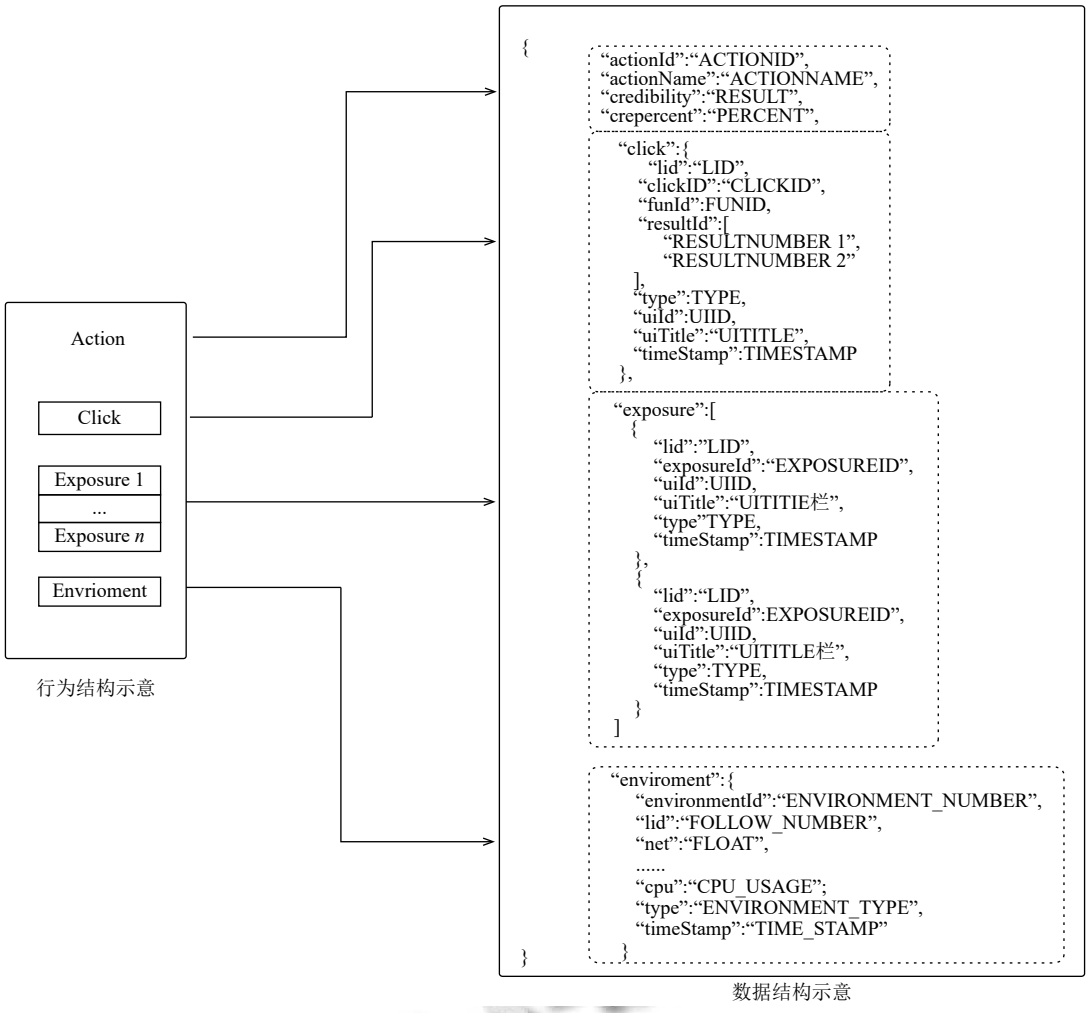


图 2 行为声明中“行为”的结构示意图

1.2 融入测试工具

在软件开发阶段接入可信测试工具, 如图 3 所示是以 Linux 为例的测试包结构. 通用结构包括三部分: 接口模块, 埋点模块, 校验模块. 接口模块主要作用是向下封装, 向上提供入口. 埋点模块主要作用是在行为发生, 在软件的反馈动作路径上会触发埋点上报信息给服务端, 服务端会对事件进行可信判定. 校验模块主要作用是校验软件及模块本身是否被篡改.

1.3 埋点上报

埋点在指安插在软件动作路径中的标记工具. 每当软件按照程序设定发生行为时, 特定位置埋点就会被触发, 按照规则将该程序事件信息上报给判定系统[13]. 埋点模块的目的, 记录软件行为引发的埋点事件, 从而做到动作路径有迹可循, 为之后可信判定做依据.

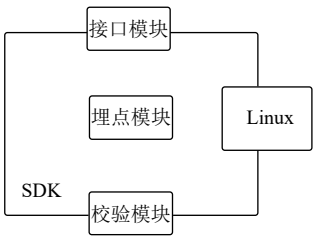


图 3 SDK 示意图

在 1.1 节中的行为声明 Action 中, 已经提到了关于程序事件的三种类型, 即点击事件、曝光事件和环境事件. 如图 4 中所示.

当一个行为发生时埋点的工作流程如图 5 所示. 首先, 埋点模块根据关键字 event-Id 去请求埋点数据源已获得埋点的详细. 然后, 埋点模块获得到埋点的详细信息, 根据埋点的类型去判断对关联标识的操作, 如果是点击事件则根据 Unix 时间戳与 event-Id 组合生成唯一的关联标识, 并携带. 如果是曝光事件或者环境事件则会直接读取关联标识, 并携带. 最后, 埋点模块将处理过的数据上传给服务端.

1.4 埋点数据的解析

如图 6 所示, 服务端向客户端提供三个接口用来分别接受三种不同类型的埋点事件, 客户端的埋点模块会自动识别事件类型然后将数据发到指定接口. 服务端在接收到数据后会按照以下流程对数据进行解析.

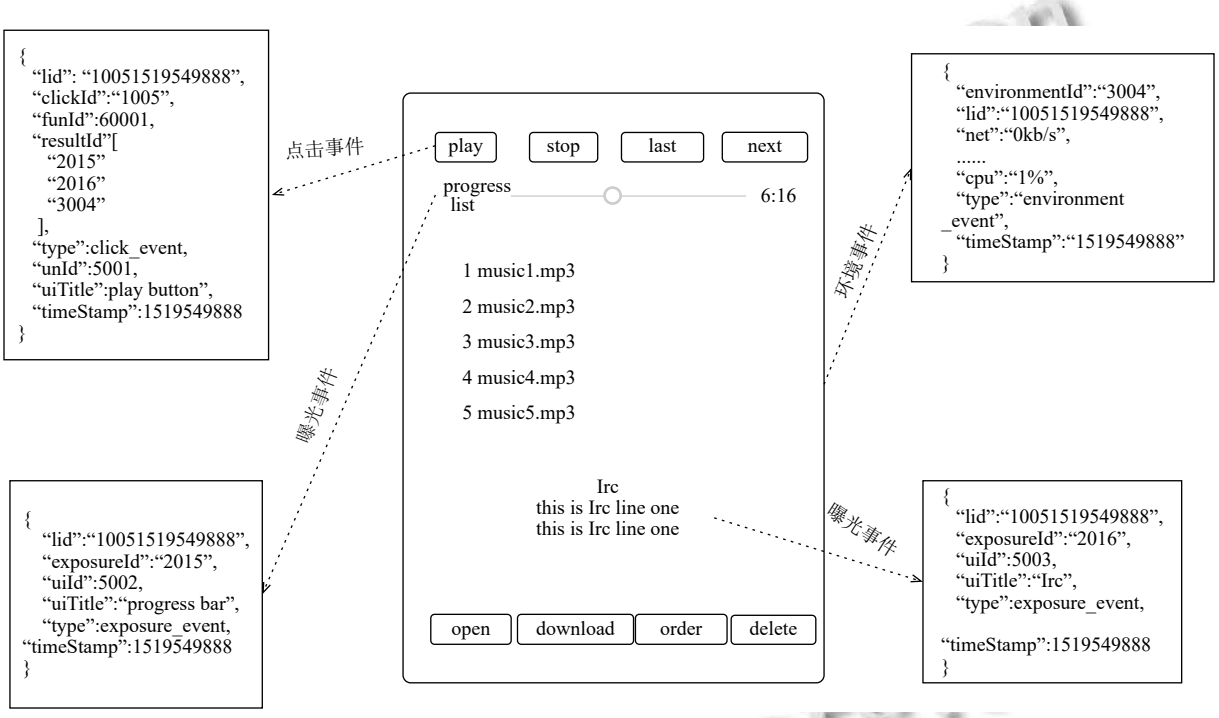


图 4 埋点样例

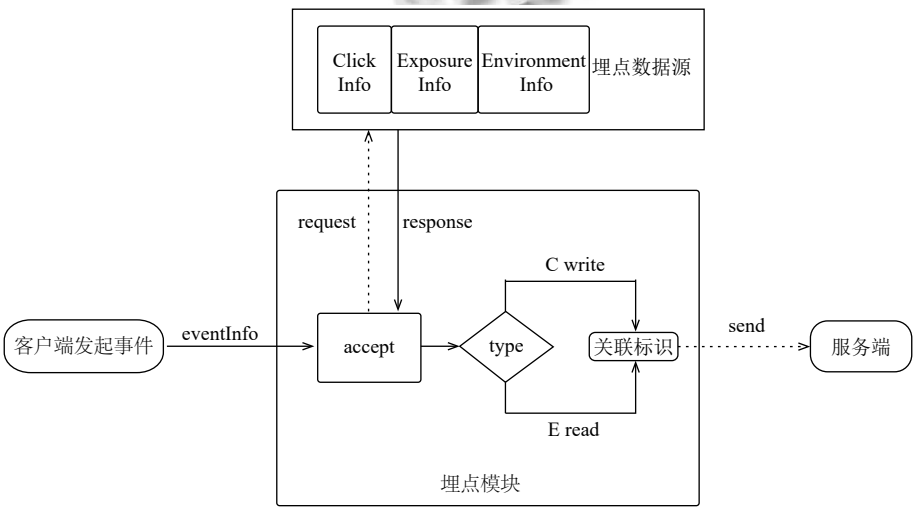


图 5 埋点工作流程

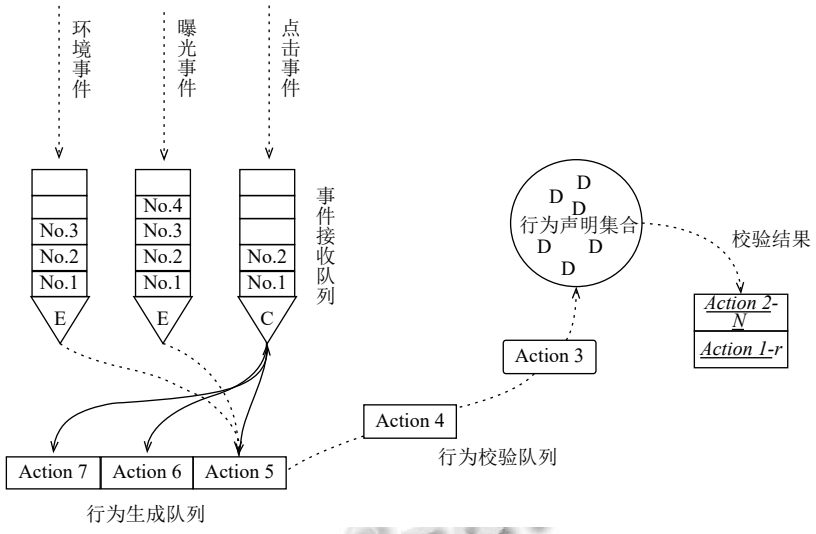


图 6 服务端解析数据示意图

首先, 将接收到的 JSON 格式数据解析成事件对象, 之后放入事件队列. 事件队列是服务端用来存放埋点事件的容器. 三个事件队列用来存放对应的三种埋点事件, 在每个队列中会根据事件到达先后顺序排序, 保证先进先出的相对顺序.

然后, 因点击事件作为动作路径开始标志, 也就是行为开始的标志, 点击事件队列会最先进行出队操作. 每当有点击事件出队时, 就代表有一个行为已经发生. 那么行为生成队列会生成一个 Action 对象用来承载该行为. 刚刚出队的点击事件会被该 Action 对象持有, 点击事件所携带的关联标识会被赋予给该行为对象 Action, 供后续携带相同关联标识的曝光事件和环境事件找到该 Action 对象并被其持有. 同时点击事件中的 result 关键字也将作为 event 匹配到所在 Action 对象的依据. 所谓行为生成队列换句话说, 就是承载这些 Action 对象的集合.

之后, 曝光事件和环境事件会像点击事件一样, 进入对应的事件队列, 然后出队, 然后根据自身携带的关联标识找到对应的 Action 对象, 并被持有. 这样就完成了一个 Action 中埋点事件的组合. 这样完整的 Action 对象就可以代表一条动作路径, 代表一个软件行为了.

最后, 服务端会读取行为声明文件, 将行为声明解析成声明队列, 即声明集合. 等待行为队列组合完毕后, 依次将行为队列出队与声明比对, 即通过埋点获得的 Action 对象与行为声明对象 Declare 对象比对. 以此, 来判定行为是否可信.

2 可信度计算的方法

2.1 可信判定指标

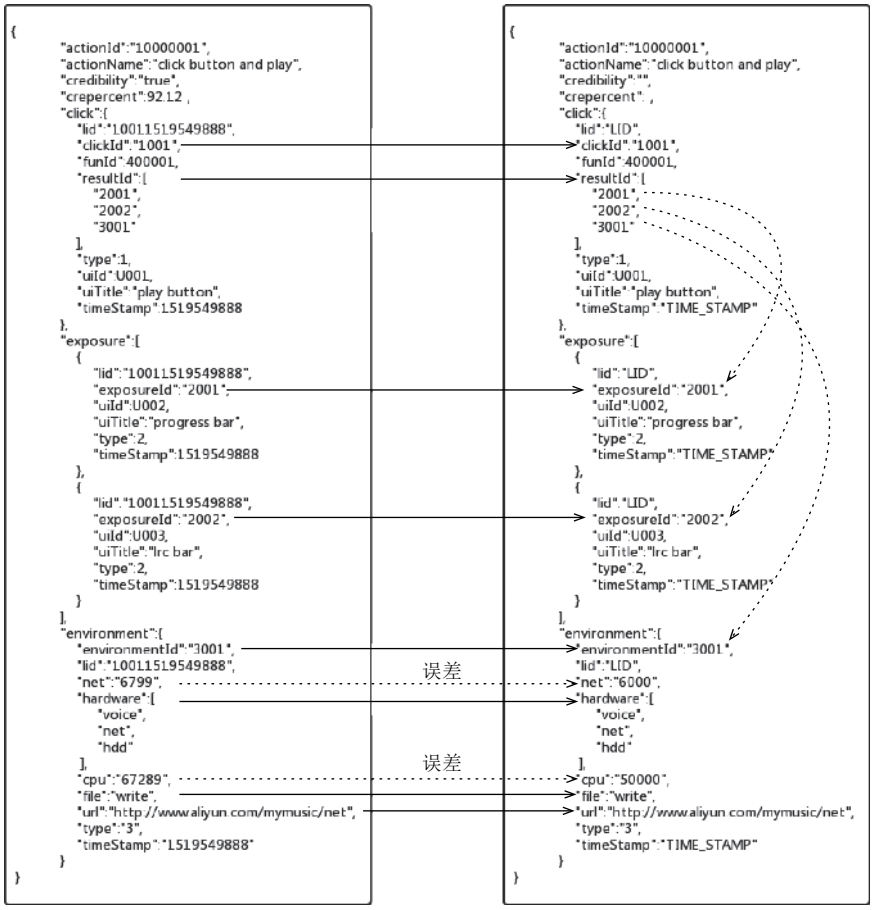
本方法提出将可信判定指标划分为显性指标和隐性指标.

显性指标是指软件动作路径的匹配, 即 Action 中的三种埋点事件的触发是完全与行为声明中一致的. 举例说明, 如图 7(b) 所示为行为声明中对点击按钮播放网络音乐的行为的 JSON 表示. 可见, 在“言”的 Action 中, 点击事件为动作路径的开始, 根据 click 中的 resultID 可知, 预期将会触发 eventID 为“2001”, “2002”, “3001”的埋点 (如图 7(b) 中右侧虚线所示). 显性指标就是比较实验监控到的 Action 中的 event 是否与行为声明中 Action 的 event 一致.

其次, 隐性指标指环境事件的系统相关参数, 比如程序对内存的使用率, 对网络的使用情况等. 设置隐性指标的目的在于检测程序是否存在欺瞒上报, 即在行为的动作路径中不触发埋点, 或者发生的实际行为与埋点不符等. 为了监控这类行为, 在客户端的测试模块中, 会在事件上报时自动填充的系统环境数据, 以此来达到检测异常的目的. 如图 7 中虚线标记的就是隐性指标.

可信判定的标准将从显性指标无误与隐性指标正常两个方面制定. 行为要首先满足显性指标无误, 再满足隐性指标在正常范围内, 才会判定为可信行为. 如图 7 中的实线箭头所示, 比较“言”与“行”中的事件是否一致. 完全一致则进行隐性指标的判断, 将在下一节阐述

隐性指标的计算方法. 若不一致, 则当即终止判定, 该行为不可信. 如图 8 所示.



(a) 实验中实际行为 (b) 行为声明中行为

图 7 可信判定标准示意图

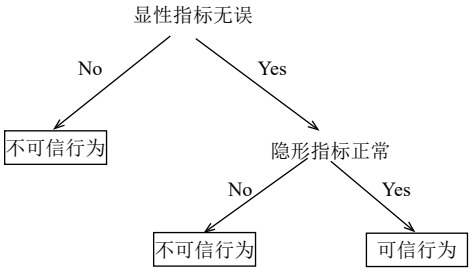


图 8 判定流程示意图

2.2 隐性指标模型与可信度计算

隐性指标是随环境事件 (环境事件) 上报的系统相关参数, 目的是用于监控实验程序发生行为时, 对系统环境的使用度. 以此对软件行为的可信判定做辅助测评. 理论上同一软件行为对系统的使用度应该是相同的, 但在实际环境中因软件自身的操作或系统环境的实时性会造成误差. 隐性指标模型是抽象出来的解析隐性指标数据的方法, 目的就是确定误差范围, 以及根据误差范围对测试样本可信度进行计算.

隐性指标模型运用 K-means 算法, 并加入可信度计算规则. 模型构造的流程如下:

(1) 通过对样本行为进行多次实验, 得到样本行为的隐性指标数据集合, 下文称之为样本集.

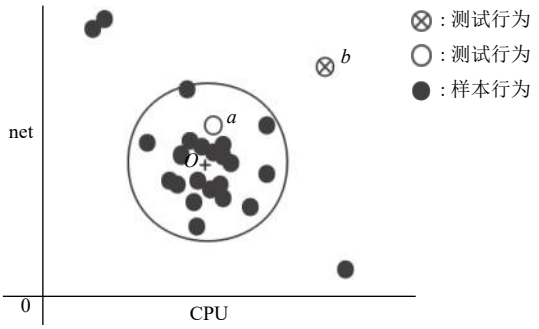
(2) 在样本集中根据欧式距离就算样本集的中心质点 O'.

(3) 以 O'为中心去除样本集中的噪点, 之后再次计算得样本中心质点 O.

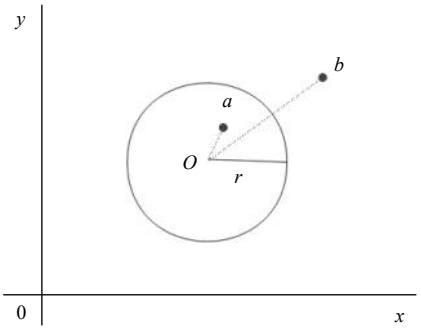
(4) 以 O 为中心, 样本集中最远样本数据的欧式距离为半径的范围即是样本行为的隐性指标模型.

实验中选取程序对内存的使用量和网络访问流量

这两个参数作为隐性指标模型的特征值, 构造的二维模型示意图如图 9(a) 所示. 可见, 圆 O 是样本行为的数据集, 样本数据集中在圆心附近, 圆外的样本数据为误差范围较大的噪点.



(a) 二维模型示意图



(b) 坐标系中示意图

图 9 可信度计算示意图

在隐性指标模型中, 可见, 可信行为样本数据点都集中在圆心 O 附近. 若我们用 $t(a, b)$ 表示点 b 在以 a 为质心的模型中的可信度. 那么我们规定: 质心 O 上的数据点可信度 $t(o, o)$ 为 100.00%; 可信度随距离圆心的距离增大而减小; 以模型边缘距离 R 为可信阈值, 边缘上的数据点可信度表示为 $t(o, r)$, 该阈值可动态设定. 模型内的数据可信度为高度可信, 外部的数据点可信度为弱度可信, 小于 0.00% 的为不可信. 如图 7(a) 中, 测试行为数据点 a 在圆内, 为高度可信; 测试行为数据点 b 在圆外且接近 $2R$, 则可信度接近 0.00% 为弱度可信.

可信度计算方法由显性因子 f 与隐性指标模型数学抽象而来. 显性因子是表示显性指标是否无误, 1 代表满足显性指标要求, 0 代表不满足显性指标要求, 显性因子具有决定性作用.

隐形指标模型数学抽象以二维数据为例, 如图 9(b) 所示. 在图中以 O 为圆心, r 为半径的圆是样本行为的数据范围. 采用欧式距离表示数据点间距离, 如下表示 16 个参数特征下 O 点与 x 点的距离是:

$$d(o,x)=\sqrt[2]{(o_1-x_1)^2+\cdots+(o_{16}-x_{16})^2} \tag{1}$$

已知圆心 O 的可信度为 $t(o, o)$, 规定圆边缘 r 的可信度为 $t(o, r)$. 若求任意数据点的可信度, 可由单位距离下的可信度一致推导. 如下所示:

$$\frac{d(o,r)}{t(o,r)}=\frac{d(o,x)}{t(o,x)} \tag{2}$$

进一步得:

$$t(o,x)=\frac{d(o,x)}{d(o,r)}*t(o,r) \tag{3}$$

引入 f 表示具有决定作用的显性因子以及质心的最高可信度 $t(o, o)$. 那么点 x 的可信度 $t(o, x)$ 就可表示为:

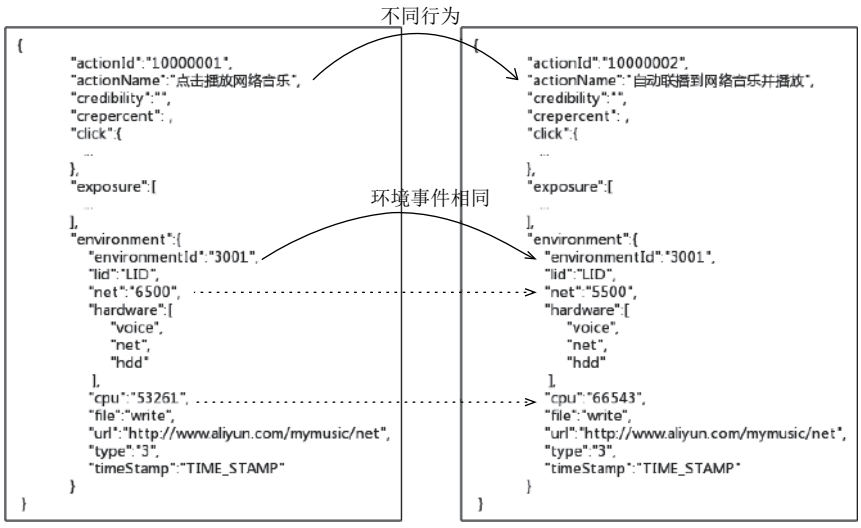
$$t(o,x)=f*\left(t(o,o)-\frac{d(o,x)}{d(o,r)}*t(o,r)\right) \tag{4}$$

2.3 相似行为可信甄别

相似行为定义为: 在软件行为的动作路径中, 会触发相同的环境事件 (环境事件) 的两个行为为相似行为. 即两个行为的动作路径中, 或者触发的点击事件和曝光事件不同, 但都以相同的环境事件. 比如图 10 所示, 图 10(a) 表示点击按钮播放播放网络音乐的 JSON. 图 10(b) 表示音乐列表自动联播到网络音乐的 JSON. 图 10(a) 和图 10(b) 表示不同的行为, 但是都会触发 environment-Id 为 3001 的播放音乐环境事件. 此环境事件中包括网络流量, 硬件支持, 内存使用, 文件读写, 网络访问域名等参数. 两个环境事件的除了隐形指标有波动外, 其余参数均相同. 这样这两个行为就为相似行为.

相似行为的可信甄别是把相同环境事件下的隐性指标相似作为依据, 运用隐性指标模型对相似行为作出可信判断, 看行为中是否存在期满动作致使隐性指标异常情况. 比如, 在播放音乐的同时, 偷偷将本地文件上传但未上报该事件. 这样会使网络流量增加, 内存占比增高. 通过埋点模块可以监控到隐性指标的波动, 由此甄别出相似行为是否可信.

如图 11 所示, 相同的环境事件 (环境事件)D, E, F 分别是隶属于三个不同行为 Action. 可知这三个行为因环境事件相同而是相似行为. 引入隐性指标模型后, D 的数据集与 E 的数据集大部分重合, 而 F 的数据集只有边缘重合. 则可判定 F 所属的行为有很大概率存在期满动作未上报.



(a) 行为-点击播放网络音乐 (b) 行为-自动联播到网络音乐并播放

图 10 相似行为

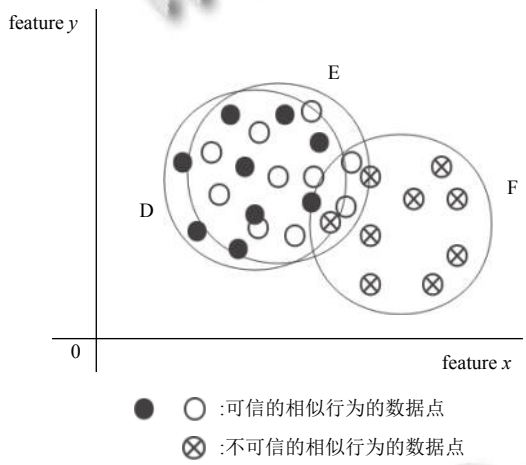


图 11 事件甄别示意图

在相似行为的可信度计算上, 其实是比较 A, B 两个行为的隐性指标数据集的重合度. 依据单个测试数据点对样本数据集可信度, 我们将问题转化为 B 中的每一个数据点对 A 数据集的可信度之和的平均数. 这样就得到了 A, B 两个相似行为的可信度. 那么可以表示为:

$$T(\mathrm{A},\mathrm{B})=\sum_{n=1}^{N}\frac{t(\mathrm{A},\mathrm{B}_n)}{n} \tag{5}$$

若 A 为可信行为, 那么 T(A, B) 即为 B 相对于 A 的可信度. 以此计算, 达到相似行为甄别的效果.

3 验证方法可行性

3.1 可信度计算分析

实验案例的客户端选取在 Linux 中运行实验程序音乐播放器来完成, 选取 8 个具有代表性的行为, 分别是播放音乐, 暂停, 切换歌曲, 打开文件和文件夹, 拖动进度条以及下载歌曲. 实验程序涉及文件读取, 硬件调用, 网络访问, 内存占用等与系统相关的交互操作, 已达到实验的功能性覆盖标准. 对三种事件类型覆盖全面, 涉及的环境事件中的参数全面, 且有相似行为, 可供相似行为甄别分析. 服务端选取 Spring MVC 架构的 Java 服务器支持, 可以提供稳定的接口支持, 访问的并发处理, 以及数据解析能力.

首先利用样本行为制造可信行为的隐性指标模型. 其次, 对可信行为进行重复实验, 查看利用本方法得到的可信度是否准确[14]. 接着, 在可信行为中加入其它行为, 且隐瞒上报, 由此制造出对应的 8 组不可信行为. 最后对 8 组不可信行为进行重复实验, 查看可信度是否准确. 在此展示选取的 5 次实验的结果, 如表 1 所示.

由此表得出, 对环境事件影响较小的行为, 在可信度计算中的可信度都达到了 0.9 以上. 对环境事件波动较大的下载行为, 可信度在 0.68~0.90 之间.

在对不可信行为的构造中, 有两种情形. 第一, 对动作路径的破坏, 即发生非预期行为, 触发非预期埋点事件, 造成显性指标的异常. 根据上文定义的可信度计

算公式, 这一种情况会直接判定可信度为 0. 第二, 是对环境事件的破坏, 即发生期满上报的行为, 导致环境参数异常, 造成隐形指标模型计算可信度下降. 不可信行为的 5 组数据如表 2 所示, 其中 Action 的括号里内容为对行为的异常处理.

表 1 实验中可信行为的 5 组可信度

Action	Test 1	Test 2	Test 3	Test 4	Test 5
播放音乐	0.96	0.95	0.99	0.90	0.89
暂停	0.99	0.99	0, 98	0.98	0.97
切换上一首	0.89	0.87	0.86	0.92	0.93
切换下一首	0.94	0.98	0.94	0.95	0.91
打开文件	0.99	0.98	0.96	0.97	0.93
打开文件夹	0.91	0.95	0.93	0.94	0.91
拖动进度条	0.88	0.87	0.93	0.89	0.90
播放网络歌曲	0.80	0.83	0.78	0.68	0.77

表 2 实验中不可信行为的 5 组可信度

Action	Test 1	Test 2	Test 3	Test 4	Test 5
播放音乐 (欺瞒下载)	0.10	0.07	0.11	0.09	0.13
暂停 (欺瞒下载)	0.12	0.13	0.09	0.15	0.21
切换上一首 (跳跃两首)	0	0	0	0	0
切换下一首 (音量增大)	0.45	0.56	0.39	0.67	0.45
打开文件 (欺瞒下载)	0.05	0.10	0.12	0.03	0.16
打开文件夹 (暂停播放)	0	0	0	0	0
拖动进度条 (停止播放)	0	0	0	0	0
播网络歌曲 (错误地址)	0	0	0	0	0

由表 2 中数据可以看出, 对显现指标为达到标准的行为, 测试方法能准确的判定为可信度 0.在欺瞒行为的可信度计算上, 对环境事件影响较大的行为, 可信度在 0.2 以下. 对环境事件影响较小的事件, 可信度在 0.45~0.67 之间.

3.2 相似行为甄别分析

在相似行为的分析上选取播放音乐 (行为 A), 切换上一首 (B) 和切换下一首 (C) 三个行为做比对, 为了增加系统参数, 我们默认三种行为均会连接网络下载歌词以及歌曲. 此三个行为都会触发事件 ID 为 3001 的播放环境事件.

可信的相似行为的验证上, 选取对三个行为分别进行多次试验, 构造出三个不同的隐性指标模型, 进而再利用本文提出的相似度计算方法得出相似行为的可信度.

在参数上的选择上, 我们选取 UI 帧率, UI 响应时间, 点击响应时间, 硬件响应时间, 文件写入量, 读取量, 当前内存使用量, 交换区总量, CPU 用户使用率, 系统使用率, 当前等待率, 当前错误率, 当前空闲率, 接收的总包裹数, 发送的总包裹数, 连接时长, 这 16 个指标作为本次实验的隐性指标.

分别对三种行为进行 50 次实验. 以行为 A 为例构造的数据矩阵示意图如图 12 所示.

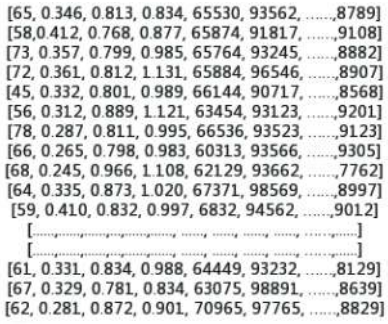


图 12 数据示意图

将 A 行为的数据矩阵 Matix 录入 K-means 收敛程序. 根据上文提出的方案, 降噪处理后, 依据中心质点 M. 根据公式 (4) 和公式 (5), 已知可信中心点与可信半径 r, 将 B 行为逐条录入计算可信度取平均值, 即得到 B 对 A 的可信相似度为 0.835, 相对 C(切换上一首) 相似度为 0.811. 对 C 行为做欺瞒处理 (网络下载歌曲) 后, 用同样方式测得相似度为 0.231. 有明显的数据波动, 由此说明相似行为的可信判断是具有可行性的.

4 结论

本论文中可信测试方法重点解决了两个方面的问题, 第一是在软件运行的过程中通过埋点感知软件行为的动作路径. 第二是将埋点信息重组软件行为机制, 依据行为声明做比较, 提出针对隐形指标的的 K-means 可信度的计算模型, 并应用于相似行为的可信甄别. 在计算模型的应用上, 环境事件波动越大准确度越高, 在对环境事件影响小的行为上, 准确度有待提高. 这也是后续值得改进的地方.

参考文献

1 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展. 中国科学: 信息科学, 2010, 40(2): 139–166.
2 沈国华, 黄志球, 谢冰, 等. 软件可信评估研究综述: 标准、模型与工具. 软件学报, 2016, 27(4): 955–968. [doi: 10.13328/j.cnki.jos.005024]
3 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述. 中国科学 E 辑: 信息科学, 2007, 37(2): 129–150.

4 Yu XJ, Jiang GZ, Wang P, *et al*. Research on application's credibility verification based on ABD. Wuhan University Journal of Natural Science, 2016, 21(1): 63–68. [doi: 10.1007/s11859-016-1139-8]
5 吕海庚. 基于行为声明软件可信性测试方法的研究[硕士学位论文]. 北京: 北京工业大学, 2016.
6 车乐林. 基于行为声明的移动应用可信性测试的研究与应用[硕士学位论文]. 北京: 北京工业大学, 2017.
7 刘妙晨. 基于行为声明的 REST 风格软件可信性测试的研究与应用[硕士学位论文]. 北京: 北京工业大学, 2017.
8 韩冬冬, 韩永飞, 张俊华. 应用软件可信性混合度量的设计和应用. 电脑与信息技术, 2013, 21(3): 31–33, 45. [doi: 10.3969/j.issn.1005-1228.2013.03.011]
9 熊刚, 兰巨龙, 胡宇翔, 等. 基于可信度量的网络组件性能评估方法. 通信学报, 2016, (3): 117–128.
10 赵玉洁, 罗新星. Web 软件可信性的模糊评价方法. 计算机应用研究, 2014, 31(4): 1072–1076. [doi: 10.3969/j.issn.1001-3695.2014.04.028]
11 綦磊升, 张晓娜, 门星火, 等. 基于模糊层次分析法的指挥信息系统仿真试验可信性评估. 软件工程, 2018, 1(1): 7–11.
12 Su D, Li J, Wang ZY. A method of dynamic trusted researching of software behavior and its trusted elements. Network Security Technology & Application, 2013, (4): 14–17.
13 Dugundji ER, Poorthuis A, Van Meeteren M. Modeling user behavior in adoption and diffusion of twitter clients. Proceedings of 2011 IEEE International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. Boston, MA, USA. 2011. 1372–1379.
14 Gan T, Lin FH, Chen CJ, *et al*. User behaviors analysis in Website identification registration. China Communications, 2013, 10(3): 76–81. [doi: 10.1109/CC.2013.6488832]