Time-travel Testing of Android Apps

Zhen Dong
National University of Singapore
zhen.dong@comp.nus.edu.sg

Lucia Cojocaru
Politehnica University of Bucharest
lucia.cojocaru@stud.acs.upb.ro

ABSTRACT

Android testing tools generate sequences of input events to exercise the state space of the app-under-test. Existing search-based techniques systematically evolve a population of event sequences so as to achieve certain objectives such as maximal code coverage. The hope is that the mutation of fit event sequences leads to the generation of even fitter sequences. However, the evolution of event sequences may be ineffective. Our key insight is that pertinent app states which contributed to the original sequence’s fitness may not be reached by a mutated event sequence. The original path through the state space is truncated at the point of mutation.

In this paper, we propose instead to evolve a population of states which can be captured upon discovery and resumed when needed. The hope is that generating events on a fit program state leads to the transition to even fitter states. For instance, we can quickly deprioritize testing the main screen state which is visited by most event sequences, and instead focus our limited resources on testing more interesting states that are otherwise difficult to reach.

We call our approach time-travel testing because of this ability to travel back to any state that has been observed in the past. We implemented time-travel testing into TimeMachine, a time-travel enabled version of the successful, automated Android testing tool Monkey. In our experiments on a large number of open- and closed-source Android apps, TimeMachine outperforms the state-of-the-art search-based/model-based Android testing tools Sapienz and Stoat, both in terms of coverage achieved and crashes found.

1 INTRODUCTION

Android app testing has been gaining in importance. In 2020, there is a smart phone for every third person (2.9 billion users) while app revenue will double from 2016 (US$ 88 to 189 billion).1 The number of bugs and vulnerabilities in mobile apps is growing. In 2016, 24.7% of mobile apps contained at least one high-risk security flaw [1]. The Android testing market is also expected to double in five years from US$ 3.21 billion in 2016 to US$ 6.35 billion in 2021.2

To illustrate the challenges of existing Android testing tools, take for example Super Metroid (Fig. 1), one of the best games for the NES gaming console, now available for Android. Super Metroid is played on a large map of rooms that can be explored in any order. By pushing the right buttons on the controller, the main character Samus moves from one room to the next, finding secrets and gaining in strength by fighting enemies. Today, Android app testing is like playing a game of Super Metroid, albeit without the ability to save after important milestones and to travel back in time when facing the consequences of a wrong decision.

One possible approach is to generate a single, very long sequence of events in a random fashion [3]. However, the testing tool may ultimately get stuck in dead ends. For instance, Samus may fall into pits or get lost in a particularly complex part of the labyrinth. This problem is overcome only partially by restarting the Android app because (i) we must start from the beginning, (ii) there is no clean slate, e.g., database entries remain, and (iii) how to detect when we are stuck is still an open question. For Android testing, the ability to save and travel back to the most interesting states goes a long way towards a more systematic exploration of the state space.

Another Android app testing approach [36] is to evolve a population of event sequences in a search-based manner. In each iteration, the fittest event sequences are chosen for mutation to generate the next generation of event sequences. An event sequence is mutated because of this ability to travel back to any state that has been observed in the past. We implemented time-travel testing into TimeMachine, a time-travel enabled version of the successful, automated Android testing tool Monkey. In our experiments on a large number of open- and closed-source Android apps, TimeMachine outperforms the state-of-the-art search-based/model-based Android testing tools Sapienz and Stoat, both in terms of coverage achieved and crashes found.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ACM ISBN 978-1-4503-7121-6/20/05...
https://doi.org/10.1145/3377811.3380402

In this paper, we propose instead to evolve a population of states which can be captured upon discovery and resumed when needed. By capturing and resuming an app’s states, we seek to achieve a systematic state space exploration (without going to the extent of exhaustive exploration as in formal verification). Due to the ability to travel back to any past state, we call this as time-travel testing. Our novel time-travel testing approach systematically resets the entire system—the Android app and all of its environment—to the most progressive states that were observed in the past. A progressive state is one which allows us to discover new states when different input events are executed. Once the tool gets stuck, it goes back in time and resumes a progressive state to execute different events.

We implement time-travel testing for Android apps into TimeMachine—a time-travel-enabled variant of the automated Android testing tool Monkey [3]. In our example, one can think of TimeMachine as an automatic player that explores the map of Super Metroid through very fast random actions, automatically saves after important milestones, and once it gets stuck or dies, it travels back to secret passages and less visited rooms seen before in order to maximize the coverage of the map. Compared to tools that evolve event sequences, such as Sapienz [36], TimeMachine does not mutate the sequence prefix which is required to reach the fittest, most progressive state, and instead generates only the sequence suffix starting from that state. Compared to tools that generate a single, very long event sequence, such as Monkey [3] or Stoat [40], TimeMachine automatically detects when it gets stuck (i.e., there is a lack of progress) and resumes that state for further testing which is most promising for finding errors. In our experiments with Sapienz, Stoat, and Monkey on both open-source and closed-source Android apps TimeMachine substantially outperformed the state-of-the-art in terms of both, coverage achieved and errors found.

TimeMachine can be seeded with a set of initial event sequences. At the beginning of a testing session, TimeMachine takes a snapshot of the starting state. During test execution, TimeMachine takes a snapshot of every interesting state and adds it to the state corpus, travels back to the interesting state and executes the next test. For each transition from one state to another, TimeMachine also records the shortest event sequence. If no initial test set is provided, TimeMachine only adds the starting state to the state corpus.

TimeMachine is an automatic time-travelling-enabled test generator for Android apps that implements several heuristics to choose the most progressive state from the state corpus to explore next. Intuitively, a state reaching which covered new code and that has been difficult to reach has more potential to trigger new program behavior. TimeMachine dynamically collects such feedback to identify the most progressive state. TimeMachine identifies a progressive state as one which itself was infrequently visited and the k nearest neighbors were visited relatively infrequently.

Our experiments demonstrate a substantial performance increase over our baseline test generation tool—Monkey extended with system-level event generator of Stoat [40]. Given the 68 apps in the AndroTest benchmark [23], our time-travel strategy enables the baseline tool to achieve 1.15 times more statement coverage and to discover 1.73 times more unique crashes. Given 37 apps in the benchmark of industrial apps, around 900 more methods are covered on average and 1.5 times more unique crashes are discovered. Our time-travel strategy makes TimeMachine so efficient that it outperforms the state-of-the-art test generators Sapienz [36] and Stoat [40] both in terms of coverage as well as errors found, detecting around 1.5 times more unique crashes than the next best test generator. TimeMachine tested the Top-100 most popular apps from Google Play and found 137 unique crashes.

In summary, our work makes the following contributions:

• We propose time-travel testing for Android which resumes the most progressive states observed in the past so as to maximize efficiency during the exploration of an app’s state space. The approach identifies and captures interesting states as save points, detects when there is a lack of progress, and resumes the most progressive states for further testing. For instance, it can quickly deprioritize the main screen state which is visited by most sequences, and resume/test difficult-to-reach states. We propose several heuristics that guide execution to a progressive state when progress is slow.

• We implement the time-travel testing framework and an automated, feedback-guided, time-travel-enabled state space exploration technique for Android apps. The framework and testing technique are evaluated on both open-source and closed-source Android app benchmarks, as well as top-100 popular apps from Google Play. We have made our time-travel Android app testing tool TimeMachine publicly available on Github: https://github.com/DroidTest/TimeMachine

2 TIME-TRAVEL FRAMEWORK

We design a general time-travel framework for Android testing, which allows us to save a particular discovered state on the fly and restore it when needed. Figure 2 shows the time-travel infrastructure. The Android app can be launched either by a human developer or an automated test generator. When the app is interacted with, the state observer module records state transitions and monitors the change of code coverage. States satisfying a predefined criteria are marked as interesting, and are saved by taking a snapshot of the entire simulated Android device. Meanwhile the framework observes the app execution to identify when there is a lack of progress, that is, when the testing tool is unable to discover any new program behavior over the course of a large number of state transitions. When a “lack of progress” is detected, the framework terminates the current execution, selects, and restores the most progressive one among previously recorded states. A more progressive state is one that allows us to discover more states quickly. When we travel back to the progressive state, an alternative event sequence is launched to quickly discover new program behaviors.

The framework is designed as easy-to-use and highly-configurable. Existing testing techniques can be deployed on the framework by implementing the following strategies:

• Specifying criteria which constitute an “interesting” state, e.g., increases code coverage. Only those states will be saved.

• Specifying criteria which constitute “lack of progress”, e.g., when testing techniques traverse the same sequence of states in a loop.

• Providing an algorithm to select the most progressive state for time-travelling when a lack of progress is detected.
2.1 Taking Control of State

State identification. In order to identify what constitutes a state, our framework computes an abstraction of the current program state. A program state in Android app is abstracted as an app page which is represented as a widget hierarchy tree (non-leaf nodes indicate layout widgets and leaf nodes denote executable or displaying widgets such as buttons and text-views). A state is uniquely identified by computing a hash over its widget hierarchy tree. In other words, when a page’s structure changes, a new state is generated.

To mitigate the state space explosion problem, we abstract away values of text-boxes when computing the hash over a widget hierarchy tree. By the above definition, a state comprises of all widgets (and their attributes) in an app page. Any difference in those widgets or attribute values leads to a different state. Some attributes such as text-box values may have huge or infinite number of possible values that can be generated during testing, which causes a state space explosion issue. To find a balance between accurate expressiveness of a state and state space explosion, we ignore text-box values for state identification. Our practice that a GUI state is defined without considering text-box values is adopted by previous Android testing works as well [21, 22].

State saving & restoring. We leverage virtualization to save and restore a state. Our framework works on top of a virtual machine where Android apps can be tested. A virtual machine (VM) is a software that runs a full simulation of a physical machine, including the operating system and the application itself. For instance, a VM with an Android image allows us to run Android apps on a desktop machine where related hardware such as the GPS module can be simulated. App states can be saved and restored with VM.

Our framework records a program state by snapshotting the entire virtual machine state including software and emulated hardware inside. States of the involved files, databases, third-party libraries, and sensors on the virtual device are kept in the snapshot so that the state can be fully resumed by restoring the snapshot. This overcomes the challenge that a state may not be reached from the initial state by replaying the recorded event sequence due to state change of background services.

2.2 Collecting State-Level Feedback

To identify whether a state is “interesting”, our framework monitors the change in code coverage. Whenever a new state is generated, code coverage is re-computed to identify whether the state has potential to cover new code via the execution of enabled events. Our framework supports both open-source and close-source apps. For open-source apps, we collect statement coverage using the Emma coverage tool [9]. For closed-source, industrial apps, we collect method coverage using the Ella coverage tool [8]. For closed-source apps, statement coverage is difficult to obtain.

Our framework uses a directed graph to represent state transitions, where a node indicates a discovered state and an edge represents a state transition. Each node maintains some information about the state: whether there is a snapshot (only states with snapshots can be restored), how often it has been visited, how often it has been restored, and so on. This information can be provided to testing tools or human testers to evaluate how well a state has been tested and to guide execution.

3 METHODOLOGY

We develop the first time-travel-enabled test generator TimeMachine for Android apps by enhancing Android Monkey [3] with our framework. TimeMachine’s procedure is presented in Algorithm 1. TimeMachine’s objective is to maximize state and code coverage. TimeMachine starts with a snapshot of the initial state (lines 1-4). For each event that Monkey generates, the new state is computed and the state transition graph updated (lines 5-9). If the state isInteresting (Sec. 3.1), a snapshot of the VM is taken and associated with that state (lines 10-13). If Monkey isStuck and no more progress is made (Sec. 3.2), TimeMachine finds the most progressive state (selectFittestState; Sec. 3.3) and restores the associated VM snapshot (lines 14-17). Otherwise, a new event is generated and loop begins anew (lines 5-18).

3.1 Identifying Interesting States

TimeMachine identifies an interesting state based on changes in GUI or code coverage (Line 10 in Algorithm 1). The function isInteresting(state) returns true if (1) state is visited for the first time, and (2) when state was first reached new code was executed.
Algorithm 1: Time-travel testing (TimeMachine).

Input: Android App, Sequence generator Monkey
1. State curState ← LAUNCH(App)
2. Save VM snapshot of curState
3. Interesting states states ← {curState}
4. State Transition Graph stateGraph ← INITGRAPH(curState)
5. for each Event e in Monkey.GENERATEEVENT() do
6. if timeout reached then break; end if
7. prevState ← curState
8. curState ← EXECUTEEVENT(App, e)
9. stateGraph ← UPDATEGRAPH(prevState, curState)
10. if ISINTERESTING(curState, stateGraph) then
11. Save VM snapshot of curState
12. states ← states ∪ {curState}
13. end if
14. if isSTUCK(curState, stateGraph) then
15. curState ← SELECTFITTESTSTATE(states, stateGraph)
16. Restore VM snapshot of curState
17. end if
18. end for
Output: State Transition Graph stateGraph

The intuition behind our definition of "interesting" states is that the execution of new code provides the evidence that a functionality that has not been tested before is enabled in the discovered state. More new code related to the functionality might be executed by exploring this state. For instance, suppose clicking a button on screen S1 leads to a new screen S2, from where a new widget is displayed (increasing code coverage). The new widget comes with its own event handlers that have not been executed. These event handlers can be covered by further exploring screen S2. This heuristic not only accurately identifies an interesting state (S2 in this case) but also significantly reduces the total number of saved states (since only interesting states are saved during testing).

3.2 Identifying Lack of Progress

The testing process can stay unprogressive without discovering any new program behavior for quite some time. As reasons for Monkey getting stuck, we identified loops and dead ends.

Loops. A loop is observed when the same few (high-frequency) states are visited again and again. To easily perform routine activities, app pages are typically organized under common patterns, e.g., from the main page one can reach most other pages. This design leads to a phenomenon where random events tend to trigger transitions to app pages which are easy to trigger. Moreover, apps often browse nested data structures, it is difficult to jump out from them without human knowledge. For example, let us consider the AnyMemo [7] app, a flashcard learning app we tested. Monkey clicks a button to load a CSV file and arrives at an app page that browses system directories. It keeps on exploring directories and cannot leave this app page until it finds a CSV file to load (or by pressing the "Back" button many times in a row). In our experiments, Monkey could not jump out of the loop within 5000 events.

Dead ends. A dead end is a state which is difficult to exit. Some pages require specific inputs which are very unlikely to be randomly generated. Monkey can be trapped by them and can keep on generating events without making any "progress". For instance, consider an app page in AnyMemo [7] where a form needs to be filled and submitted. Yet, the "Submit" button is located at the bottom of the page, and does not even appear on screen. Monkey would need to correctly fill in certain parameters, scroll all the way to the bottom, and then generate a "Click" event on the button to transition to exit the page. This is quite unlikely. Monkey gets stuck in a dead end.

When TimeMachine gets stuck, the most progressive state is traveled back to (lines 14-17 in Algorithm 1). The function isSTUCK is sketched in Algorithm 2 and realizes a sliding window algorithm. Firstly, four parameters must be specified, which are explained later. There are two global variables, a queue of specified length l and a counter which keeps track how often the same state has been observed (lines 1-3). Given the current app state and the state transition graph, if the current state is the same as the previous state the no-progress counter is incremented (lines 4-7). Otherwise, the counter is reset (lines 8-11). If the counter exceeds the specified maximum (maxNoProgress), then a dead end is detected (lines 12-14). If the fixed-length queue is filled and the proportion of "easy" states in the queue surpasses the specified threshold β, then a loop is detected. Two kinds of states in the queue are considered easy: states occurring multiple times in the queue, and states among the top α percentage of the most frequently visited states.

Algorithm 2: Detecting loops and dead-ends (isSTUCK).

Input: Queue length l
Input: Lack-of-progress threshold maxNoProgress
Input: Max. top (α · 100%) most frequently visited states
Input: Max. proportion β of repeated plus frequent states
1: FIFO Queue ← empty queue of length l
2: noProgress = 0 // #events since last state transition
3: for l, then break; end if
4: procedure isSTUCK(State curState, Graph stateGraph)
5: prevStateID = Queue.top()
6: if prevStateID == curState.ID then
7: noProgress ← noProgress + 1
8: else
9: Queue.push(curState.ID)
10: noProgress = 0
11: end if
12: if noProgress > maxNoProgress then
13: return true // detect dead ends
14: end if
15: if Queue.length == l then
16: nRepeated ← countMaxRepeatedStates(Queue)
17: nFrequent ← countFreqStates(Queue, stateGraph, a)
18: if (nRepeated + nFrequent)/l > β then
19: return true // detect loops
20: end if
21: end if
22: return false
23: }
ADB Daemon transitions. The with two Android versions. that arereach-workswith the of a on Android are all states implementation. also includes a system-level event TimeMachine is computed according to Equation (1). With this algorithm, $f \leftarrow f + 3$. For each $f$, bestFitness $0$ do from $f$. end if. In our experiments, we let $k = 3$. For each interesting state, TimeMachine computes the average fitness of a state in the $k$-neighborhood of the state. The state with the maximum average state fitness in its $k$-neighborhood is returned. The $k$-neighborhood of state are all states $s$ in stateGraph that are reachable from state along at most $k$ transitions. The fitness $f(s)$ of a state $s$ is computed according to Equation (1). With this algorithm, Monkey not only travels in time to the state with the highest fitness value but also continues to explore states with high fitness values within $k$ transitions, which maximizes the benefit of time travel.

4 IMPLEMENTATION

Our time travel framework is implemented as a fully automated app testing platform, which uses or extends the following tools: VirtualBox [4], the Python library pyvbox [11] for running and controlling the Android-x86 OS [6], Android UI Automator [10] for observing state transitions, and Android Debug Bridge (ADB) [5] for interacting with the app under test. Figure 3 gives an architectural overview of our platform. Components in grey are implemented by us while others are existing tools that we used or modified.

For coverage collection, our framework instruments open-source apps using Emma [9] (statement coverage) and closed-source apps using Ella [8] (method coverage). Ella uses a client-server model sending coverage data from the Android OS to the VM host via a socket connection. Unfortunately, this connection is broken every time a snapshot is restored. To solve this issue, we modified Ella to save coverage data on the Android OS to actively pull as needed.

On top of the time travel framework, we implement TimeMachine. To facilitate the analysis of all benchmarks, we integrated TimeMachine with two Android versions. TimeMachine works with the most widely-used version, Android Nougat with API 25 (Android 7.1). However, to perform end-to-end comparison on AndroTest benchmark [23], we also implement TimeMachine on Android KitKat version with API 19 (Android 4.4). The publicly available version of Sapienz [36] (a state-of-the-art/practice baseline for our experiments) is limited to Android API 19 and cannot run on Android 7.1. To collect state-level feedback, we modified Android Monkey and UI Automator to monitor state transition after each event execution. TimeMachine also includes a system-level event generator taken from Stoat [40] to support system events such as phone calls and SMSs.

5 EMPIRICAL EVALUATION

In our experimental evaluation, we seek to answer the following research questions.

![Figure 3: Architecture of TimeMachine implementation.](Image 433x674 to 454x704)
RQ1: How effective is our time-travel strategy in terms of achieving more code coverage and finding more crashes? We compare TimeMachine to the baseline into which it was implemented.

RQ2: How does time-travel testing (i.e., TimeMachine) compare to state-of-the-art techniques in terms of achieved code coverage and found crashes?

RQ3: How does time-travel testing (i.e., TimeMachine) perform on larger, real-world apps, such as industrial apps and Top-100 apps from Google Play?

5.1 Experimental Setup

To answer these research questions, we conducted three empirical studies on both open-source and closed-source Android apps.

Study 1. To answer RQ1, we evaluate TimeMachine and baseline tools on AndroTest [23] and investigate how achieved code coverage and found faults are improved by using the time-travel strategy. We chose AndroTest apps as subjects because AndroTest has become a standard testing benchmark for Android and has been used to evaluate a large number of Android testing tools [16, 20, 23, 34–37, 40, 44]. It was created in 2015 by collecting Android apps that have been used in evaluations of 14 Android testing tools.

TimeMachine applies time-travel strategy to a baseline tool; the baseline tool is Monkey extended with Stoat’s system-level event generator. To accurately evaluate effectiveness of time-travel strategy, we set Monkey extended with the system-level event generator from Stoat as baseline (called MS). We chose MS instead of Monkey as a baseline tool to make sure that the improvement achieved by TimeMachine completely comes from time-travel strategy, not from system event generation.

We also implement another variant of Monkey as baseline to evaluate effectiveness of “heavy components” such as state saving and restoring on enhancing a test technique. This variant applies only the lack of progress detection component of our time-travel strategy without state saving and restoring components. When lack of progress is detected, it simply restarts testing from scratch, i.e., re-launching app under test without resuming states (called MR).

In TimeMachine, parameters $l$, $max0Progress$, $\alpha$, $\beta$ for isStuck in Alg. 2 are set to 10, 200, 0.2, and 0.8, respectively. These values were fixed during initial experiments of two authors with three apps from AndroTest (Anymemo, Bites, aCal). We executed these apps with Monkey for many rounds and recorded relevant data such as the number of state transitions when a loop was observed and the number of executed events when Monkey jumped out from a dead end. Based on observed data and authors’ heuristics, we came up with several groups of values and evaluated them on these three apps, and eventually chose above data as default parameter values. In the evaluation, TimeMachine used the default values for all the three studies. Baseline tool MS and MR use the same parameter values as in TimeMachine.

Study 2. To answer RQ2, we evaluate TimeMachine and state-of-the-art app testing tools on AndroTest and compare them in terms of achieved code coverage and found crashes. For state-of-the-art tools, we chose Monkey [3], Sapienz [36], and Stoat [40]. Monkey is an automatic random event sequence generator for testing Android apps and has been reported to achieve the best performance in two works [23, 42]. Sapienz and Stoat are the most recent techniques for Android testing. These testing tools have also been adequately tested and are standard baselines in the Android testing literature. To have a fair comparison, all techniques use their default configuration.

Study 3. To answer RQ3, we evaluate TimeMachine, baseline tools and all state-of-the-art techniques on large real-world Android apps, and investigate whether they have a consistent performance on both closed-source and open-source Android apps. In this evaluation, we use IndustrialApps [42] as subject apps. IndustrialApps was a benchmark suite created in 2018 to evaluate the effectiveness of Android testing tools on real-world apps. The authors sampled 68 apps from top-recommended apps in each category on Google Play, and successfully instrumented 41 apps with a modified version of Ella [8]. In our experiment, we chose to use the original version of Ella and successfully instrumented 37 apps in Industrial app-suite. On this benchmark, we could not compare with Sapienz because the publicly available version of Sapienz is limited to an older version of Android (API 19).

To further investigate the usability of TimeMachine, we evaluate TimeMachine on Top-100 popular Android apps from Google Play and investigate whether TimeMachine can effectively detect crashes in online apps, i.e., those available for download from Google Play at the time of writing. Following the practice adopted by some previous authors [36, 40] of applying the technique to top popular apps on Google Play, we focus on analyzing detected crashes by TimeMachine and do not compare TimeMachine with state-of-the-art techniques on this data set. Top-100 popular apps were collected by downloading the most highly ranked apps on Google Play and instrumenting them with our coverage tool Ella until we obtained 100 apps that could be successfully instrumented by Ella.

Procedure. To mitigate experimenter bias and to scale our experiments, we chose to provide no manual assistance during testing in all studies. For all test generators, the Android testing is fully automatic. None of the test generators is seeded with an initial set of event sequences. The testing process is automatically started after installation. All data are generated and processed automatically. We neither provide any input files, nor create any fake accounts. Each experiment is conducted for six (6) hours and repeated five (5) times totalling 35580 CPU hours ($\approx$ 4.1 year). To mitigate the impact of random variations during the experiments, we repeated each experiment five times and report the average. In comparison, the authors of Sapienz report one repetition of one hour while the authors of Stoat report on five repetitions of three hours. We chose a time budget of six hours because we found that the asymptotic coverage was far from reached after three hours in many apps (i.e., no saturation had occurred).

Coverage & Crashes. We measure code coverage achieved and errors discovered within six hours. To measure statement or method coverage, we use Emma and Ella, the same coverage tools that are used in Sapienz and Stoat. To measure the number of unique crashes detected, we parse the output of Logcat,\(^5\) an ADB tool that dumps a log of system messages. We use the following protocol to identify a unique crash from the error stack (taken from Su et al. [40]):

- Remove all unrelated crashes by retaining only exceptions containing the app’s package name (and filtering others).

\(^5\)https://developer.android.com/studio/command-line/logcat
The experiments were conducted on two physical machines with 64 GB of main memory, running a 64-bit Ubuntu 16.04 operating system. One machine is powered by an Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz with 56 cores while the other features an Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz with 40 cores. To allow for parallel executions, we run our system in Docker (v1.13) containers. Each Docker container runs a VirtualBox (v5.0.18) VM configured with 2GB RAM and 2 cores for the Android 4.4 and 2 cores and 4GB RAM for Android 7.1. We made sure that each evaluated technique is tested under the same workload by running all evaluated techniques for the same app on the same machine.

5.2 Experimental Results

5.2.1 Study 1: Effectiveness of Time-travel Strategy

Table 1 shows achieved coverages and found faults by each technique on 68 Android apps. The highest coverage and most found crashes are highlighted with the gray color for each app. The results of TimeMachine and baseline techniques are shown in column "TimeMachine" and "Baselines". Recall that MS indicates Monkey extended with Stoat's system-level event generator and MR indicates Monkey with the ability to restart testing from scratch when lack of progress is detected.

Comparison between TimeMachine and MS. TimeMachine achieves 54% statement coverage on average and detects 199 unique crashes for 68 benchmark apps. MS achieves 47% statement coverage on average and detects 115 unique crashes. TimeMachine covers 1.15 times statements and reveals 1.73 times crashes more than MS. To further investigate these results, Figure 4 presents achieved code coverage over execution time for all 68 apps. As we can see, TimeMachine has achieved higher coverage from around the 20th minute onwards, finally achieving 7% more statement coverage at the end of execution time. Figure 5 presents the box-plots of the final coverage results for apps grouped by size-of-app, where "x" indicates the mean for each box-plot. We see that coverage improvement is substantial for all four app size groups.

- Given the related crash information, extract only the crash stack and filter out all information that is not directly relevant (e.g., the message "invalid text...").
- Compute a hash over the sanitized stack trace of the crash to identify unique crashes. Different crashes should have a different stack trace and thus a different hash.
Our time-travel strategy effectively enhances the existing testing technique (MS) by achieving 1.15 times statement coverage and detecting 1.73 times crashes on 68 benchmark apps.

Comparison between TimeMachine and MR. MR achieves 47% statement coverage on average and detects 45 unique crashes for 68 benchmark apps. TimeMachine achieves 1.15 times statement coverage and 4.4 times unique crashes more than MR. Similarly, Figure 4 and Figure 5 shows TimeMachine covers more code in a short time and substantially improves statement coverage for all four app size groups compared to MR. This shows that it is not sufficient to simply restart an app from scratch when lack of progress is detected, though MR improves Monkey by 3% statement coverage (Monkey’s statement coverage is shown in the third subcolumn of column “State-of-the-art” of Table 1).

State saving and restoring as well as other components substantially contribute to enhancing testing techniques, it is not sufficient to simply restart app from scratch when lack of progress is detected.

5.2.2 Study 2: Testing Effectiveness.

The results of state-of-the-art techniques are shown in column “State-of-the-art” of Table 1 (ST, SA, and MO indicate Stoat, Sapienz and Monkey, respectively). As can be seen, TimeMachine achieves the highest statement coverage on average (54%) and is followed by Sapienz (51%), Stoat (45%) and Monkey (44%). Figure 6 also shows that TimeMachine achieves the highest statement coverage for all four app size groups. TimeMachine detects the most crashes (199) as well, followed by Stoat (140), Sapienz (121) and Monkey (48).

The better results from TimeMachine can be explained as follows: state-level feedback accurately identifies which parts in app are inadequately explored. Moreover an inadequately explored state can be arbitrarily and deterministically launched for further exploration via restoring a snapshot. Existing techniques typically observe program behavior over an event sequence that often is very long and goes through many states. Coverage feedback of an individual state is unavailable. So our time travel framework enhances app testing by providing fine-grained state-level coverage feedback.

Figure 7: Comparison of total number of unique crashes for AndroTest apps. The dark grey areas indicate the proportion of crashes found by both techniques.

TimeMachine achieves the highest statement coverage and detects the most crashes on 68 benchmark apps compared to state-of-the-art techniques. Promisingly, our time-travel framework has a potential to enhance state-of-the-art app testing tools to achieve better results.

To study performance across apps, for each technique under evaluation, we compute the number of apps on which the technique achieves the best performance. In terms of statement coverage, TimeMachine achieves the best performance on 45 apps, followed by Sapienz (19 apps), Stoat (11 apps) and Monkey (1 app). For detected crashes, TimeMachine achieves the best performance on 32 apps. For Stoat, Sapienz, and Monkey, there are 16, 15, and 4 apps, respectively. We further perform a pairwise comparison of detected crashes among evaluated techniques. As shown in Figure 7, there is less than ten percent overlap between the crashes found by TimeMachine and Stoat, or TimeMachine and Sapienz, respectively. The overlap with Monkey is reasonably high. About 60% of unique crashes found by Monkey are also found by TimeMachine; however TimeMachine found many new crashes which are not found by Monkey. This analysis shows that TimeMachine can be used together with other state-of-the-art Android testing techniques to jointly cover more code and discover more crashes.

TimeMachine complements state-of-the-art Android testing techniques in terms of the ability to discover more crashes and cover more code.
Table 2: Results from 37 closed-source industrial apps.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Name</th>
<th>#Method</th>
<th>%Coverage ST MO MS MR</th>
<th>%Crashes ST MO MS MR</th>
<th>#State ST MO MS MR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoScrn24</td>
<td>49772</td>
<td>34</td>
<td>25</td>
<td>29</td>
<td>31 29</td>
</tr>
<tr>
<td>Best Hairstyles</td>
<td>28227</td>
<td>14</td>
<td>20</td>
<td>13</td>
<td>15 14</td>
</tr>
<tr>
<td>Crackle</td>
<td>48702</td>
<td>26</td>
<td>9</td>
<td>19</td>
<td>22 20</td>
</tr>
<tr>
<td>Duolingo</td>
<td>46382</td>
<td>26</td>
<td>13</td>
<td>22</td>
<td>23 22</td>
</tr>
<tr>
<td>ES File Explorer</td>
<td>47273</td>
<td>28</td>
<td>15</td>
<td>18</td>
<td>24 21</td>
</tr>
<tr>
<td>Evernote</td>
<td>45880</td>
<td>21</td>
<td>10</td>
<td>7</td>
<td>13 8</td>
</tr>
<tr>
<td>Excel</td>
<td>48849</td>
<td>20</td>
<td>9</td>
<td>14</td>
<td>14 2</td>
</tr>
<tr>
<td>Filters For Selfie</td>
<td>17145</td>
<td>17</td>
<td>8</td>
<td>9</td>
<td>9 8</td>
</tr>
<tr>
<td>Flipboard</td>
<td>41563</td>
<td>30</td>
<td>17</td>
<td>24</td>
<td>28 25</td>
</tr>
<tr>
<td>Floor Plan Creator</td>
<td>23030</td>
<td>29</td>
<td>20</td>
<td>23</td>
<td>26 26</td>
</tr>
<tr>
<td>Fox News</td>
<td>42569</td>
<td>28</td>
<td>13</td>
<td>21</td>
<td>20 17</td>
</tr>
<tr>
<td>G.P. Newspund</td>
<td>56225</td>
<td>7</td>
<td>5</td>
<td>6</td>
<td>5 5</td>
</tr>
<tr>
<td>GO Launcher Z</td>
<td>45791</td>
<td>13</td>
<td>9</td>
<td>11</td>
<td>11 12</td>
</tr>
<tr>
<td>GoodRx</td>
<td>48222</td>
<td>24</td>
<td>19</td>
<td>21</td>
<td>22 17</td>
</tr>
<tr>
<td>move flirt X</td>
<td>47271</td>
<td>16</td>
<td>18</td>
<td>10</td>
<td>12 10</td>
</tr>
<tr>
<td>LINE Camera</td>
<td>47295</td>
<td>15</td>
<td>15</td>
<td>14</td>
<td>15 15</td>
</tr>
<tr>
<td>Marvel Comics</td>
<td>43578</td>
<td>18</td>
<td>18</td>
<td>15</td>
<td>17 15</td>
</tr>
<tr>
<td>Match</td>
<td>50436</td>
<td>15</td>
<td>13</td>
<td>15</td>
<td>15 11</td>
</tr>
<tr>
<td>Merriam-Webster</td>
<td>50436</td>
<td>28</td>
<td>21</td>
<td>18</td>
<td>24 23</td>
</tr>
<tr>
<td>Mirror</td>
<td>36662</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8 8</td>
</tr>
<tr>
<td>My baby piano</td>
<td>20975</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7 7</td>
</tr>
<tr>
<td>OfficeSuite</td>
<td>45876</td>
<td>17</td>
<td>16</td>
<td>16</td>
<td>16 14</td>
</tr>
<tr>
<td>OneNote</td>
<td>50100</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>10 13</td>
</tr>
<tr>
<td>Pinterest</td>
<td>46071</td>
<td>21</td>
<td>10</td>
<td>16</td>
<td>15 8</td>
</tr>
<tr>
<td>Quzllet</td>
<td>48369</td>
<td>33</td>
<td>20</td>
<td>30</td>
<td>23 31</td>
</tr>
<tr>
<td>Singing</td>
<td>46251</td>
<td>10</td>
<td>6</td>
<td>5</td>
<td>6 8</td>
</tr>
<tr>
<td>Speedometer</td>
<td>47773</td>
<td>16</td>
<td>16</td>
<td>13</td>
<td>13 15</td>
</tr>
<tr>
<td>Spotify</td>
<td>44556</td>
<td>17</td>
<td>16</td>
<td>11</td>
<td>10 10</td>
</tr>
<tr>
<td>TripAdvisor</td>
<td>46617</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23 22</td>
</tr>
<tr>
<td>trivago</td>
<td>50879</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>14 10</td>
</tr>
<tr>
<td>Watch/SFPN</td>
<td>43639</td>
<td>26</td>
<td>22</td>
<td>23</td>
<td>25 24</td>
</tr>
<tr>
<td>Whatpad</td>
<td>44669</td>
<td>25</td>
<td>14</td>
<td>13</td>
<td>12 15</td>
</tr>
<tr>
<td>WEBTOON</td>
<td>47465</td>
<td>21</td>
<td>17</td>
<td>19</td>
<td>16 14</td>
</tr>
<tr>
<td>Wish</td>
<td>48207</td>
<td>15</td>
<td>15</td>
<td>17</td>
<td>15 14</td>
</tr>
<tr>
<td>Word</td>
<td>49999</td>
<td>186</td>
<td>9</td>
<td>14</td>
<td>14 14</td>
</tr>
<tr>
<td>Yelp</td>
<td>46903</td>
<td>24</td>
<td>16</td>
<td>17</td>
<td>17 17</td>
</tr>
<tr>
<td>Zedge</td>
<td>46799</td>
<td>24</td>
<td>23</td>
<td>22</td>
<td>23 21</td>
</tr>
<tr>
<td>Ave/Sum</td>
<td>44882</td>
<td>17</td>
<td>16</td>
<td>15</td>
<td>17 15</td>
</tr>
</tbody>
</table>

5.2.3 Study 3: Closed-source Apps.

Table 2 shows results of 37 closed-source benchmark apps. It is clear that TimeMachine achieves the highest method coverage 19% and the most found crashes 281 among all evaluated techniques. Compared to baseline MS and MR, TimeMachine improves method coverage to 19% from 17% and 15%, respectively. Note that the improvement of 2% to 4% is considerable since each app has 44182 common type is native crashes, i.e., their stack traces explicitly point to the source code. As we see in Figure 8, the tested apps are quite diverse being selected from more than 10 categories. It comes as no surprise that the majority of them are ranked with over 4 stars, and are being actively maintained.

In the 87 apps, we found 137 unique crashes. These are all non-native crashes, i.e., their stack traces explicitly point to the source code. As we see column "#State" in Table 1 and Table 2, more states are discovered in apps with rich functionality and less states are discovered in simple apps. For instance, app AnyMemo with plentiful activities has 311 found states and app Frozenbubble with few activities has 15 found states. Similar results can be found for industrial apps. Note that no login is provided in the evaluation, such that TimeMachine might identify a small number of states for some large scale apps, like K9Mail.

In total, TimeMachine detects 137 unique crashes in 25 of Top-100 Google Play apps.

5.2.4 Analysis on State Identification and Time-travel.

State identification. The evaluation shows GUI layout is appropriate to identify an app state. This state abstraction generates acceptable number of states for an app, at the same time sufficiently captures features of a state. As we see column "#State" in Table 1 and Table 2, more states are discovered in apps with rich functionality and less states are discovered in simple apps. For instance, app AnyMemo with plentiful activities has 311 found states and app Frozenbubble with few activities has 15 found states. Similar results can be found for industrial apps. Note that no login is provided in the evaluation, such that TimeMachine might identify a small number of states for some large scale apps, like K9Mail.

GUI layout sufficiently captures features of an app state. On average, 85 states are found in an open source benchmark app and 358 states are found in an industrial benchmark app.

Frequency. An automatic Android testing tool that generates a very long event sequence, like Monkey, may get stuck in loops or dead ends. We measure the number of times, our time-travelling infrastructure is employed to understand how often Monkey gets stuck. In six hours over all runs and apps, Monkey gets stuck with a mean of 305.6 and a median of 308.5 times. As we can see in the box plots of Figure 9, there are generally less restores as the number of states for some large scale apps, like K9Mail.
We realise that our results on Stoat versus Sapienz and those reported in the Stoat paper [40] are vastly different. We checked with the authors of Stoat [40] on this matter. The authors of Stoat explain the disparity (i) by additional files they provided to the Android Device via SDCard, and (ii) running of experiments at their end on a different machine (Intel Xeon(R) CPU @ 3.50Ghz, 12 cores, 32GB RAM) with hardware acceleration.

Additionally, we took two measurements to rule out crashes that might be caused by our technique itself (i.e., artificial crashes). First, TimeMachine inserted a delay of 200 ms between two events to avoid crashes due to Monkey generating many events in a very short time. Second, we manually checked stack traces to filter out crashes due to state restoring issues such as inconsistent states.

Finally, our technique tests apps in a virtual machine installed with Android-x86 OS and does not support physical devices yet. For apps interacting with a remote server, our technique saves/restores only app states without considering remote server states.

7 RELATED WORK

The stream of works most closely related to ours is that of time-travel debugging [17, 28, 29, 32, 41]. Time-travel debugging allows the user to step back in time, and to change the course of events. The user can now ask questions, such as: “What if this variable had a different value earlier in the execution”? Now, time-travel testing has a similar motivation. The tester can test the state-ful app for various, alternative sequences of events, starting in any state.

This work was originally inspired by existing work on coverage-based greybox fuzzers (CGF)[2, 18, 19, 39]. A CGF, started with a seed corpus of initial inputs, generates further inputs by fuzzing. If a generated input increases coverage, it is added to the seed corpus. Similar to CGF, our time-travel-enabled test generator maintains a state corpus with states that can be restored and fuzzed as needed.

Search-based. The most closely related automatic Android test generation techniques employ search-based methods. Mao et al. developed a multi-objective automated testing technique Sapienz [36]. Sapienz adopts genetic algorithms to optimize randomly generated tests to maximize code coverage while minimizing test lengths. EvoDroid [35], the first search-based framework for Android testing, extracts the interface model and a call graph from app under test and uses this information to guide the computational search process. Search-based approaches are easy to deploy and have attracted a lot of attention from industry, e.g., Sapienz has been used to test different kinds of mobile apps at Facebook. Our work TimeMachine takes a search-based approach as well, but instead of a population of input sequences it evolves a population of app states. Our work proposes a new perspective of app testing as state exploration, and provides a feedback-guided algorithm to efficiently explore an app’s state space.

Random. One of the most efficient approaches for testing Android apps is the random generation of event sequences [23]. Apps are exercised by injecting arbitrary or contextual events. Monkey [3] is Google’s official testing tool for Android apps, which is built into the Android platforms and widely used by developers. Monkey generates random user events such as clicks, touches, or gestures, as well as a number of system-level events. Dynodroid [34] employs a feedback-directed random testing approach with two
strategies: **BIASEDRANDOM** favors events related to the current context, and **FREQUENCY** is biased towards less frequently used events. Although random testing has gained popularity because of its ease of use, it suffers from an early saturation effect, i.e., it quickly stops making progress, e.g., no new code is executed after certain number of event executions. From this point of view, our work powers random testing with the ability to jump to a progressive state observed in the past when there is no progress. Thus, an early saturation can be avoided.

**Model-based.** Another popular approach of Android apps testing is model-based testing. App event sequences are generated according to models which are manually constructed, or extracted from project artefacts such as source code, XML configuration files and UI runtime state. Ape [26] leverages runtime information to evolve an initial GUI model to achieve more precise models. Staot [40] assigns widgets in a GUI model with different probabilities of being selected during testing and adjusts them based on feedback such as code coverage to explore uncovered models. AndrodRipper [13] uses a depth-first search over the user interface to build a model. A3E [15] explores apps with two strategies: **Targeted Exploration** which prioritizes exploration of activities that are reachable from the initial activity on a static activity transition graph, and **Depth-first Exploration** which systematically exercises user interface in depth-first order. Droidbot [30], ORBIT [44] and PUMA [27] use static and dynamic analysis to build basic GUI models from app under test, on top of which different exploration strategies can be developed. Model-based approaches have attracted a great deal of attention in this field because they allow to represent app behavior as a model on which various exploration strategies can be applied. However, complex widgets (e.g., animation) commonly-used in modern apps pose difficulties on model construction, leading to an incomplete model. Combining model-based approaches with other techniques such as random testing can be a promising option for Android apps testing.

**Learning-based.** A different line of work uses machine learning to test Android apps. Liu et al. [33] use a model learned from a manually crafted data set (including manual text inputs and associated contexts) to produce text inputs that are **relevant** to the current context during app testing. For instance, it would use a name for an existing city when generating an input for a search box if there is a nearby item labeled Weather. Wuji [45] employs evolutionary algorithms and deep reinforcement learning to discover the state space of a game under test. SwiftHand [20] uses machine learning to learn a model of the user interface, and uses this model to discover unexplored states. The technique by Degott et al. [24] leverages reinforcement learning to identify valid interactions for a GUI element (e.g., a button allows to be clicked but not dragged) and uses this information to guide execution. Humanoid [31] takes manual event sequences and their corresponding UI screens to learn a model and uses the model to predict human-like interactions for an app screen. Machine learning is typically applied to resolve specific challenge in the event sequence generation, such as generating contextual text inputs or identifying possible types of input events that can be executed upon a GUI element. In contrast, our work features a fully automated Android event sequence generator. Some components in TimeMachine such as identifying an interesting state might benefit from machine learning since learning-based approaches have shown to be effective for similar issues. It is worth exploring this direction in future work.

**Program analysis-based.** Several existing approaches employ program analysis when testing Android apps. ACTEve [14] uses symbolic execution to compute enabled input events in a given app state and systematically explores the state by triggering these events. SynthesisSE [25] leverages concolic execution and program synthesis to automatically generate models for Android library calls. CrashScope [38] combines static and dynamic analysis to generate an event sequence that is used to reproduce a crash. Similarly, IntelliDriod [43] uses static and dynamic analysis to generate an event sequence that leads execution to a specified API invocation. Thor [12] executes an existing test suite under adverse conditions to discover unexpected app behavior. Such program analysis provides detailed information about the app, which can help to guide test sequence generation. At the same time, intrinsic limitations of program analysis such as poor scalability create an impediment to easy and widely-applicable automation. In contrast, our work TimeMachine requires little information from the app under test and is widely applicable to variety of Android apps as shown by our experiments.

8 CONCLUSION

Android app testing is a well-studied topic. In this paper, we develop time-travel app testing which leverages virtualization technology to enhance testing techniques with the ability to capture snapshots of the system state—state of the app and all of its environment. Capturing snapshots facilitates our time-travel-enabled testing tool to visit arbitrary states discovered earlier that have the potential to trigger new program behavior. State-level feedback allows our technique to accurately identify progressive states and travel to them for maximizing progress in terms of code coverage and state space exploration.

Our time-travel strategy enhances a testing technique (Monkey extended with Staot’s system-level generator) by achieving 1.15 times more statement coverage and discovering 1.7 times more crashes on the AndroTest benchmark. Moreover, TimeMachine outperforms other state-of-the-art techniques (Sapienz and Staot) by achieving the highest coverage on average and the most found crashes in total. On large, industrial apps, TimeMachine covers around 900 more methods on average and discover 1.5 times more unique crashes over the baseline tool, at the same time outperforms state-of-the-art techniques as well. Our tool TimeMachine also reveals a large number of crashes, owing to a wide variety of exceptions (nine different kinds of exceptions), in real-life top popular apps from Google Play.

ACKNOWLEDGMENTS

This work was partially supported by the National Satellite of Excellence in Trustworthy Software Systems, funded by NRF Singapore under National Cybersecurity R&D (NCR) programme, and an ArRF Tier1 project T1 251RES1708 from Singapore. This research was partially funded by the Australian Government through an Australian Research Council Discovery Early Career Researcher Award (DE190100046).