ITPP0982
ICT

ARC'14
مؤتمر مؤسسة قطر السنوي للبحوث
QATAR FOUNDATION ANNUAL RESEARCH CONFERENCE
Towards World-class Research and Innovation

An Integrated Framework For Verified And Fault Tolerant Software

10.5339/qfarc.2014.ITPP0982

Samir Elloumi, Ph.d.; Ishraf Tounsi; Bilel Boulifa; Sharmeen Kakil; Ali Jaoua; Mohammad Saleh

Corresponding author :
eloumis@qu.edu.qa
Qatar University, Doha, Qatar

Abstract

Fault tolerance techniques should let the program continue servicing in spite of the presence of errors. They are of primary importance mainly in case of mission-critical systems. Their eventual failure may produce important human and economic casualties. For these reasons, researchers have assigned the software reliability as an important research area in terms of checking its design and functionality. As a matter of fact, software testing aims to increase the software correctness by verifying the program outputs w.r.t an input space generated in a bounded domain. Also, the fault tolerance approach has many effective error detection mechanisms as per as the Backward recovery, Forward recovery or redundancy algorithm. Our work consists of developing an integrated approach for software testing in a bounded domain. It tolerates transient faults to solve deficiencies and to obtain a robust and well-designed program. The developed framework comprises two types of tests: i) Semi-automatic test that enables the user to check the software by manually entering the values of the method and testing with specified values, ii) Automatic test that computerizes the test with the prepared instances of the program and generated values of a chosen method that exists inside the software. For generating the input values of a program, we have involved "Korat" that requires a class invariant, a bounded domain and Java Predicates (or preconditions). The framework uses the reflection technique in order to verify the correctness of the method under test. Based on the pre-post conditions, or Java predicates, previously fixed by the user, the backward recovery and the Forward recovery algorithm are applied to tolerate the transient faults. In case of Forward recovery, an efficient original solution has been developed based on reducing the number of re-executing a bloc of instructions. In fact, the re-execution is started from the current state instead of the initial state under the hypothesis of no loss of critical information. A plugin Java library has been implemented for fault tolerant version. The Framework was experimented for several java programs and was applied for improving the robustness of the Gas purification software.
ACKNOWLEDGMENT: This publication was made possible by a grant from the Qatar National Research Fund through National Priority Research Program (NPRP) No. 04-1109-1-174. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the Qatar National Research Fund or Qatar University