APALACHE: Abstraction-based Parameterized TLA Checker

Abstract

Modern Internet services offered by Amazon, Google, Facebook, or Netflix run in the Cloud. Client requests are served by thousands of computers that are located in datacenters that are distributed worldwide. At this scale, faults become the norm rather an exception. At the same time blockchain technology promises a new open economy that is supported by cryptography and distributed consensus. Blockchains are distributed and comprise thousands of voting computers. The promise of the blockchain technology can only be fulfilled if the blockchains are indeed fault-tolerant and cannot be compromised by individual attackers. Thus, it becomes increasingly important to design fault tolerance mechanisms in a rigorous manner, and to verify that these mechanisms indeed hold up to their promises. TLA+ is a general specification language that is used for designing distributed protocols, including fault-tolerant protocols. The language was invented by Leslie Lamport, the Turing Award Laureate of 2013. Intel, Microsoft Research, and Amazon Web Services used TLA+ to design their systems. In 2016, we started the project Apalache with the vision of developing automatic verification tools for fault-tolerant protocols that are specified in TLA+. Our main motivation was to provide the users with a verification tool that would scale better to the recent verification challenges than the standard tool TLC, which implements the classical exhaustive state enumeration techniques. Since then, we have developed the Apalache model checker that uses the state-of-the-art logic solvers (called SMT solvers) to reason about properties of TLA+ specifications. Using Apalache we can check distributed protocols whose state space is beyond the reach of exhaustive state enumeration techniques. We participate in the regular meetings of the researchers working on the TLA+ tools, organized by Leslie Lamport and including researchers from Microsoft Research, Microsoft-Inria Joint Research Centre, Inria Nancy, and our team. We are working on integration of Apalache with the TLA+ tools. Ultimately, we will integrate Apalache in TLA+ Toolbox - the integrated development environment for TLA+, which is used worldwide to design distributed systems. The typical approach to ensure correctness of a TLA+ specification for thousands of com[1]puters consists of two steps: (1) run TLC and Apalache to debug the specification for a small number of participants, and (2) formalize correctness for an arbitrary number of participants with the interactive theorem prover TLAPS. For realistic systems, this typically involves several person-month of work for a verification engineer. A fully automatic approach to (2) is called parameterized model checking. It faces many theoretical and practical limits. To address parameterization, we introduced new methods for a predominant class of fault-tolerant algorithms and implemented these new methods in our tool ByMC (Byzantine Model Checker). Our next goal is to build a bridge between Apalache and ByMC. Our results find international recognition. From a scientific viewpoint, we are invited to give lectures and tutorials in the USA, Belgium, and Malta in 2020. From an industrial viewpoint, the project leaders Igor Konnov and Josef Widder were offered to continue their research at Informal Systems Ltd. with a focus on verification of the Tendermint blockchain. We are starting this new research endeavor at the new Vienna hub of Informal Systems, which provides four employments for skilled researchers and research engineers in Vienna.

Scientific disciplines:
102022 - Software development (50%) | 102025 - Distributed systems (40%) | 101013 - Mathematical logic (10%)

Keywords:
computer-aided verification, model checking, parameterized verification,TLA+, fault-tolerant distributed algorithms

Principal Investigator:	Igor Konnov
Institution:	Vienna University of Technology
Collaborators:	Josef Widder (Vienna University of Technology) (Co-Principal Investigator)

Status: Completed (01.01.2016 - 31.12.2019) 48 months

Funding volume: EUR 539,000

Further links about the involved persons and regarding the project you can find at
https://archiv.wwtf.at/programmes/information_communication/ICT15-103