Informatik-Kolloquium

Fachgruppe Informatik

Lehrstuhl Informatik 2

RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

EINLADUNG

Zeit: Donnerstag, 15. Okt. 2009, 16.30 Uhr

Ort: AH I, Ahornstr. 55

Referentin: Prof. Dr. Marta Kwiatkowska,
University of Oxford

Titel: On Quantitative Software Verification

Abstract:

The vast majority of software verification research to date has concentrated on qualitative analysis methods, for example the absence of safety violations in program executions. Many programs, however, contain randomisation, timing and resource information. Quantitative verification is a technique for establishing quantitative properties of a system model, such as the probability of battery power dropping below minimum, the expected time for message delivery and the expected number of messages lost before protocol termination. Tools such as the probabilistic model checker PRISM (www.prismmodelchecker.org) are widely used in several application domains, including security and network protocols, but their application to real software is limited.

This lecture presents recent results concerning quantitative software verification for ANSI-C programs extended with random assignment. The goal is to focus on system software that exhibits probabilistic behaviour and properties such as “the maximum probability of file-transfer failure”, or “the maximum expected number of failed transmissions”. We use a quantitative abstraction-refinement framework based on predicate abstraction, in which probabilistic programs are represented as Markov decision processes and their abstractions as stochastic two-player games. These techniques have been implemented using components from GOTO-CC, SATABS and PRISM and successfully used to verify actual networking software.

Es laden ein: Die Dozenten der Informatik