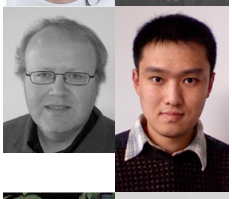
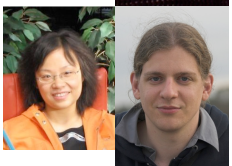
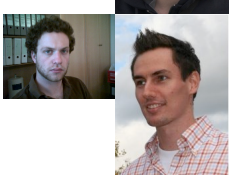
Software Modeling and Verification

Staff





- **Professors**
  - Prof. Dr. Ir. Joost-Pieter Katoen PD
  - Prof. em. Dr. Klaus Indermark
  - Prof. Dr. Erika Ábrahám
  - http://moves.rwth-aachen.de/
- **Secretary**
  - Elke Ohlenforst
- **Lecturer**
  - AOR Priv.-Doz. Dr. Thomas Noll
- **Researchers**
  - Dr. Henrik Bohnenkamp
  - Xin Chen, M.Sc.
  - Dr. Tingting Han
  - Dipl.-Inform. Jonathan Heinen
  - Dipl.-Inform. Nils Jansen
  - Dr. Carsten Kern
  - Dipl.-Inform. Daniel Klink
  - Dipl.-Inform. Ulrich Loup
  - Dr. Etienne Lozes
  - Alexandru Mereacre, M.Sc.
  - Dipl.-Inform. Martin Neuhäußer
  - Viet Yen Nguyen, M.Sc.
  - Dr. Stefan Rieger
  - Dipl.-Inform. Haidi Yue
- **Technical Staff**
  - Arnd Gehrmann

- **Diploma/Master Students**
  - M. Bretsch
  - S. de Carolis
  - F. Fiedler
  - R. Grossman
  - C. Hapsari Ayuningtyas
  - C. Jansen
  - S. Herting
  - M. Kampschulte
  - M. Odenbrett
  - S. von Styp-Rekowski
  - P. Richter

- **Student Researchers**
  - M. Brockschmidt
  - B. Bruetsch
  - F. Dulat
  - C. Dehnert
  - D. Guck
  - F. Gretz
  - C. Kuhl
  - F. Korzilius
  - M. Maass
  - M. Sarej
  - M. Scheffler
  - V. Serebro
  - C. Xu

- **Visiting Scientists**
  - Tim Albu (Fraunhofer Institut for Lasertechnik, D)
  - Dr. Pieter Collins (CWI, NL)
  - Muhammad Fadlisyah (University of Oslo)
  - Marijn Jongerden (University of Twente, NL)
  - Prof. Dr. Bengt Jonsson (Uppsala University, S)
  - Natali Kalinnik (Albert-Ludwigs-University, D)
  - Prof. Dr. Barbara König (University of Duisburg-Essen, D)
  - Prof. Dr. Marta Kwiatkowska (Oxford University, UK)
  - PD Dr. Martin Leucker (TU München, D)
  - Daniela Lepri (University of Oslo)

Dr. Etienne Lozes (ENS Cachan, F)
Dr. Larissa Meinecke (Macquarie University, Sydney)
Dr. Anne Remke (University of Twente, NL)
Dr. Julien Schmaltz (Radboud University Nijmegen, NL)
Thomas Sturm (Universidad de Cantabria, SP)
Tino Teige (University of Oldenburg, D)
Daniel Wagner, (Imperial College, UK)
Dr. Michael Weber (University of Twente, NL)
Ralf Wimmer (Universität Freiburg, D)
Dr. Ivan Zapreev (CWI, NL)
Dr. Lijun Zhang (Universität Saarland)

Overview

In 2009, significant progress has been made in the international project Quasimodo, an EU FP7 project on the quantitative verification of embedded systems, and COMPASS, a project funded by the European Space Agency (ESA). Within the context of Quasimodo, major advances in the theory of probabilistic model checking have been achieved. Amongst others, important progress has been made on two long outstanding problems: verifying continuous-time probabilistic models against linear-time probabilistic specifications, and determining the optimal policy for time-bounded reachability probabilities in continuous-time Markov decision processes. These results form the basis for numerous new research challenges.

In the COMPASS project, together with the Italian research institute FBK (the group of Alessandro Cimatti) and the French company Thales Alenia Space (one of the leading companies in satellites), we are in the second year to convince the ESA that formal methods are pivotal to model and analyze both correctness and efficiency aspects of aerospace systems. A true and interesting challenge indeed. This spring a first prototypical tool was well-received by the ESA and at the time of writing this introductory, several students and assistants are active in realizing the final toolset which will be extensively tested by Thales Alenia Space. The toolset supports the automated verification of AADL models that are extended with timed, hybrid, and probabilistic error aspects. This is an important step towards bridging the gap between engineering languages (such as AADL) and mathematically rigorous verification. At ETAPS'09, we organized an international workshop with participation of e.g., the NASA Laboratory JPL, on COMPASS-related issues. Scientific results of the COMPASS project have been presented at several international conferences and events.

In the context of the Research Training Group ALGOSYN, we have worked on compositional abstraction techniques for nondeterministic and probabilistic models. First results show the enormous benefits of applying aggressive abstraction in a component-wise manner. Other activities in ALGOSYN concern parameter synthesis of stochastic models and the verification of hybrid systems.

Besides the above running projects, the junior research group "Theory of Hybrid Systems" of E. Ábrahám, embedded in the "Software Modeling and Verification" group, started new activities in different fields. The three main research topics are (1) the analysis and the state space representation for hybrid systems, (2) counterexample generation for probabilistic systems, and (3) SMT-solving for the real algebra and its application in hybrid system verification. We established international cooperation with several research institutes working in the above fields, and applied for fundings.

Last but not least, we took part in, and also initiated some events for the motivation, support, and information of pupils interested in computer science. The Cybermentor project, which we support with out participation, aims at mentoring female pupils interested in mathematics, natural sciences, computer science, and technology. We co-organized the pupil's university (Schüleruniversität) 2009. We also started the development of a sequence of videos informing teenagers about the contents of computer science.

2009 was a very successful year in terms of successful completions of doctoral studies. Three PhD students at the MOVES chair received their PhD degree. Carsten Kern successfully defended his dissertation on "Learning of Communicating and Nondeterministic Automata" on the last day of August, Stefan Rieger did the same in September with a thesis on "Verification of Pointer Programs", and finally, Tingting Han defended her dissertation both

in Twente and in Aachen, on "Diagnosis, Synthesis, and Analysis of Probabilistic Systems" in October. All dissertations were happily approved by national and international examiners.

The are happy to report on the three highly motivated PhD student Nils Jansen, Ulrich Loup, and Xin Chen who started their PhD studies 2009 in the junior research group.

We kindly welcome Dr. Etienne Lozes (ENS Cachan), an expert on calculi for mobile systems and heap-manipulating programs, to our chair. Funded by an Alexander von Humboldt grant, Etienne will stay at the MOVES group for 18 months as a visiting professor.

The steering commitees of the international conferences QEST (Quantitative Evaluation of Systems, www.qest.org) and CONCUR (Concurrency Theory) have accepted our offer to organize these conferences as a joint event in the Super C building in September 2011. The possibility to host these two renowned conferences in Aachen can be seen as a recognition of the contributions of our CS department to these fields in the last decades.

Finally, we like to mention the enormous productivity and creativity of the researchers at the chair. Various high-quality papers have been produced, and important scientific advances have been achieved. An enormous effort has been made to handle the substantial teaching load, and all managerial and administrative issues.

It's an extremely enjoyable endeavour and very stimulating to work with such an active and talented team!

Joost-Pieter Katoen.

Research Projects

QUPES: Verification of Quantitative Properties of Embedded Software

T. Han, J.-P. Katoen, M. Neuhäußer

Embedded software typically executes on devices that, first and foremost, are not personal computers. Due to its embedded nature, its robustness is of prime importance, and timely reactions to stimuli from its -- mostly physical -- environment are essential. The aim of the QUPES project is to assess these quantitative aspects (e.g., timeliness and robustness) as an integral part of the embedded software validation phase.

To accomplish this, probabilistic model-checking techniques can be applied for models that are equipped with randomness and variants thereof which also exhibit nondeterminism. Based on efficient numerical methods and abstraction techniques, quantitative properties can be checked automatically even on large state space with millions of states using dedicated tools. Oppose to, amongst others, the essential feature of model checking, where evidences will be provided on a property refutation, counterexamples generation in probabilistic model checking is almost not developed. We provide the theoretical and algorithmic foundations for counterexample generation in probabilistic model checking, in particular for discrete-time Markov chains. One of the key principles is the casting of the concepts of strongest evidence and smallest counterexample as (variants of) shortest path problems. This enabled the use of efficient and well-studied graph algorithms for counterexample generation. These results can be extended to Markov chains with rewards, to Markov decision processes (MDPs), to LTL model checking, and have been recently been adopted in probabilistic counterexample-guided abstraction-refinement (CEGAR) techniques for MDPs as well as in counterexample generation for continuous-time Markov chains (CTMC) and cpCTL logic. Compact representation of a counterexample by regular expressions are also studied.

Further, compositional reasoning is a key strategy in analyzing complex systems as it allows the use of hierarchical and modular modeling formalisms like stochastic process algebras, stochastic activity networks or generalized stochastic Petri nets. Continuous-time Markov Decision processes (CTMDPs) are the nondeterministic counterpart of the aforementioned CTMCs and are well suited for compositional verification techniques. We define stochastic logics (like CSL) on CTMDPs and provide their measure-theoretic basis. Further, well-known equivalences like strong and weak bisimulation relations are adapted to CTMDPs which considerably reduce the state-space needed for quantitative analysis.

Verifying Pointer Programs with Unbounded Heap Structures

J. Heinen, J.-P. Katoen, Th. Noll, S. Rieger, R. Grossmann, C. Jansen

The incorrect use of pointers is one of the most common sources of software errors. This especially applies to concurrent systems whose nondeterministic behavior rises additional challenges. Proving the correctness of concurrent pointer-manipulating programs with unbounded heap, let alone algorithmically, is a highly non-trivial task. This project attempts to develop automated verification techniques and accompanying tool support for concurrent programs with dynamic thread creation and memory allocation that handle linked data structures which are potentially unbounded in their size.

In a first project phase, we concentrated on (possibly cyclic) singly-linked list data structures. A pointer logic for specifying heap properties with linear-time (LTL) operators for reasoning about system executions was developed, and finitary abstractions for the dynamic creation of both heap cells and processes were investigated. This framework supports the validation of temporal properties addressing absence of memory leaks, dereferencing of null pointers, dynamic creation of cells, and simple and position-dependent aliasing for list-manipulating programs.

Subsequently, the approach was extended to analyze programs that handle more complex dynamic data structures. We developed a novel abstraction framework that is based on graph grammars, more precisely context-free hyperedge replacement grammars, as an intuitive formalism for abstractly modeling dynamic data structures. The key idea is to use the replacement operations which are induced by the grammar rules in two directions. By a backward application of some rule, a subgraph of the heap can be condensed into a single nonterminal edge, thus obtaining an abstraction of the heap. By applying rules in forward direction, certain parts of the heap which have been abstracted before can be concretized again, which avoids the necessity for explicitly defining the effect of pointer-manipulating operations on abstracted parts of the heap. Again a temporal logic was employed to specify program properties.

This technique was successfully applied to dynamic data structures such as doubly-linked lists, binary and ternary trees (also with connected leafs), and red-black-trees. In particular, after implementing a prototype tool is was possible to establish the termination, correctness, and completeness of the well-known Deutsch-Schorr-Waite traversal algorithm in a fully automatic way.

Current focus is on improving the usability of the framework. As graph grammars for abstracting realistic heap data structures tend to become very large, developing them by hand is a complex and error-prone procedure. One promising approach that we follow is to adopt learning techniques to automatically derive abstraction grammars for the data structures occurring in the given program. Another strand of research concentrates on analyzing the (backward) confluence properties of graph grammars, which guarantees the uniqueness of abstractions.

Formal Models of Microcontroller Systems

Th. Noll, B. Schlich (i11), J. Brauer (i11)

Embedded systems usually operate in uncertain environments, giving rise to a high degree of nondeterminism in the corresponding formal models. This, together with other effects, leads

to the well-known state-space explosion problem, meaning that the models of those systems grow exponentially in size as the number of components increases. Careful handling of nondeterminism is therefore crucial for obtaining efficient tools for analysis and verification.

The goal of this project, carried out in close cooperation with the Embedded Software Laboratory of our department, is to develop formal computation models and state-space reduction techniques to tackle this problem. A first approach was taken by defining a general automata-based model for microcontrollers, taking into account both the hardware, the software, and the environment of the system. This model was used to prove the correctness of a particular abstraction method, called delayed nondeterminism, which resolves the uncertainties caused by undetermined input values only if and when this is required by the application code. More concretely, a simulation relation between the concrete and the abstract state space was established, thus showing the soundness of delayed nondeterminism with respect to "path-universal" verification logics such as ACTL and LTL. Current efforts concentrate on refining this technique using interval-based approaches.

Another source of nondeterminism is the potential occurrence of interrupts. Aiming at reducing the number of program locations where interrupt handlers have to be considered, a reduction technique was developed and proven correct which further reduces the state space that needs to be inspected. The effectiveness of this abstraction was demonstrated in several case studies.

Correctness, Modeling and Performance of Aerospace Systems (COMPASS)

Joint project together with the groups of Alessandro Cimatti (Fondazione Bruno Kessler, Centre for Scientific and Technological Research, Trento, Italy), and Xavier Olive (Thales Alenia Space, On Board Software Department, Cannes, France)

In this project we develop a model-based approach to system-software co-engineering which is tailored to the specific characteristics of critical on-board systems for the space domain. The approach is supported by a System-Level Integrated Modeling (SLIM) Language in which engineers are provided with convenient ways to specify a.o. nominal hardware, as well as software operations, timed and hybrid behavior, (probabilistic) faults and their propagation, error recovery and degraded modes of operation. This language is strongly based on AADL and its Error Model Annex which allows for the modeling of error behavior. A kernel of the SLIM language is equipped with a formal semantics that provides the interpretation of SLIM specifications in a precise and unambiguous manner. Systems are considered as a hierarchy of (hardware and software) components where components are defined by their type (interface) and implementation. Components communicate via ports allowing for message and continuous communication. The internal structure of a component implementation is specified by its decomposition into subcomponents, together with their HW/SW bindings and their interaction via connections over ports. Component behavior is specified by a textual description of mode-transition diagrams. System reconfiguration is supported by mode-dependent presence of subcomponents and their connections. Error behaviour is described by probabilistic finite state machines, where error delays may be governed by continuous random variables.

Correctness properties, safety guarantees, and performance and dependability requirements are specified using requirement specification patterns which act as parameterized ``templates'' to the engineers and thus offer a comprehensible and easy-to-use framework for requirement specification.

The properties are checked on the SLIM specification using formal analysis techniques such as model checking and probabilistic variants thereof. The precise character of these techniques and the SLIM semantics yield a trustworthy modeling and analysis framework for system and software engineers. The formal analysis is based on state-of-the-art model checking techniques such as bounded SAT-based and symbolic model checking, and extensions of model checking with numerical and simulative means to reason about quantitative requirements such as performance and dependability. The analysis facilities support, among others: automated derivation of dynamic (i.e., randomly timed) fault trees, FMEA tables, assessment of FDIR, and automated derivation of diagnosability requirements.

The prototype of an integrated platform on top of state-of-the-art tools with an accompanying graphical user interface is available, and has been evaluated by Thales Alenia Space using several case studies studying critical on-board computer-based systems from the satellite domain. Another outcome of the project is a proposal for possible extensions of AADL, its Error Model Annex and the corresponding semantics, which are currently under investigation by the AADL standardization bodies. More information on the project is available at http://compass.informatik.rwth-aachen.de/.

Quasimodo

H. Bohnenkamp, H. Yue, J.-P. Katoen

The MOVES group participates in the European research project ‘Quasimodo’, funded by the European Commission under the IST framework programme 7 for Information and Communication Technology, ICT.

The objective of the Quasimodo project is to develop theory, techniques and tool components for handling quantitative (e.g. real-time, hybrid and stochastic) constraints in model-driven development of real-time embedded systems. Ultimate aim is to increase the competitiveness of European industrial companies which develop, implement and deploy embedded systems.

More specifically, the project aims are:

1. Improving the modelling of diverse quantitative aspects of embedded systems.
2. Providing a wide range of powerful techniques for analysing modelswith quantitative information and for establishing abstraction relations between them.
3. Generating predictable code from quantitative models.
4. Improving the overall quality of testing by using suitable quantitative models as the basis for generating sound and correct test cases.
5. Applying the techniques to real-life case-studies and disseminating the results to industry.

Project partners are universities, research institutes, and companies in Germany, The Netherlands, Denmark, Belgium, and France.

The MOVES Group is currently working on a case-study for a sensor-network gossiping protocol, which is posed by one of the industrial partners.

The MoDeST Tool Environment

H. Bohnenkamp, H. Yue, J.-P. Katoen

The specification language MoDeST covers a wide spectrum of modelling concepts, ranging from plain labelled transition systems to stochastic systems like Generalised Semi-Markov Decision Processes. MoDeST possesses a rigid, process-algebra style semantics, and yet provides modern and flexible specification constructs. MoDeST specifications constitute a coherent starting-point to analyse distinct system characteristics with various techniques, e.g., model checking to assess functional correctness and discrete-event simulation to establish the system's reliability. Analysis results thus refer to the *same* system specification, rather than to different (and potentially incompatible) specifications of system perspectives like in the UML.

The tool MOTOR (MoDeST Tool enviRonment) is aimed to provide the means to analyse and evaluate MoDeST specifications. The tool is written in the C++ programming language. The tool provides (i) interfacing capabilities for connection to existing tools for specific projected models, and (ii) also means for enhancement by *native* algorithms for analysis of (classes) of MoDeST specifications. In earlier work, MOTOR has been connected to MöñBIUS, a performance evaluation tool suite that has been developed at the University of Illinois at Urbana-Champaign, US. The MoDeST/Mobius tandem is currently used and constantly improved in the Quasimodo project case-studies.

Formal Timed Testing in an Industrial Context

H. Bohnenkamp, C. Weise (i11), R. Mitsching (i11)

Testing is one of the most natural, intuitive and effective methods to increase the reliability of software. Formal methods have been employed to analyse and systematise the testing idea in general, and to define notions of correctness of implementations w.r.t. specifications in particular.

I cooperation with the company Scheidt & Bachmann in Moenchengladbach we work on a case study in the area of railway signaling and station management. Our goal is to gain experience on the problems that arise when applying a formal testing theory in practice. Ultimately we plan

to develop a methodology which meets industrial requirements for application of the formal testing approach on a daily basis in real projects.

Part of this project is the development of a testing tool for timed testing, which is based on the tiocoM testing theory. Work is in its early stages.

This project is in cooperation with i11.

Ultra High Speed Mobile Information and Communication

H. Bohnenkamp, J.-P. Katoen, H. Yue

Energy consumption is a core feature of the wireless networks which is receiving more and more attention in research. Three distinct levels for analysis of energy consumption can be identified which are strongly related but provide different abstraction levels: signal processing

level, radio link level, network level (operation as well as deployment planning). Our mean is model checking technique and our goal is to provide insight to theoretical bounds on the energy consumption at any of these three levels and minimize the energy consumption of the network. More precisely, given a protocol or an algorithms, after making some necessary simplifying assumptions regarding the system models and scenarios considered, we can model it in an appropriate model checker (e.g. PRISM, SPIN, MRMC or UPPAAL, etc.). By applying probabilistic model checking technique, we can then not only verify quantitative or qualitative properties (e.g. is it deadlock free?) of diverse network but also predict some network features with respect to energy consumptions. For example, in the field of radio network, what is the expected value of energy consumption to elect a leader. In contract to simulation based techniques, model checking explores the whole system states and hence provide theoretical soundness.

Cybermentor

E. Ábrahám

This project aims at keeping female pupils interested in the MINT sciences (mathematics, computer science, natural sciences, technology). The female teenagers (mentees), get a female mentor assigned, who supports her with clarifying informations and helpful suggestions for their choice of study. We support the project with our participation.

Other Activities

J.-P. Katoen

- Member of the Steering Committee of ETAPS (European Joint Conferences on Theory and Practice of Software).
- Member of the Steering Committee of FORMATS (Formal Methods and Analysis of Timed Systems)
- Member of the Steering Committee of QEST (Quantitative Evaluation of Systems).
- Board Member of the Dutch Society on Theoretical Computer Science (NVTI).
- Senior member of the Association of Computing Machinery (ACM)
- Member of the Program Committee of the following events: FORMATS 09, PSI 09, SOFSEM 09, YR-CONCUR 09.
- Invited speaker at:
    - Nordic Workshop on Programming Theory
    - IFIP WG 2.2 on Programming Concepts and Methodology
    - CDC Workshop on Stochastic Hybrid Systems
- Member of the IFIP Working Group 1.8 on Concurrency Theory.
- Member of the EPSRC Review College (Engineering and Physical Sciences Research Council), UK.
- Member of the NWO Computer Science Evaluation (VENI) Commitee..
- Organizer of the CONCUR Workshop for Young Researchers, Bologna, Italy, September 2009.
- Guest Professor at MacQuarie University, Sydney, Australia, March 2009.
- Co-organizer of the ETAPS Workshop on Correctness, Modeling and Performance of Aerospace Systems, York, March 2009.
- Member of several external PhD committees.

Th. Noll

- Program committee member of the 4th International Workshop on Systems Software Verification (SSV 2009)
- Program committee member of the 3rd IEEE International Conference on Secure System Integration and Reliability Improvement (SSIRI 2009)
- Program committee member of the 2nd IEEE International Conference on Secure System Integration and Reliability Improvement (SSIRI 2008)
- Member of the examination boards for CS Bachelor and Master
- Student advisor for the following applied subjects within CS: Electrical Engineering, Civil Engineering, and Medicine
- Organization of teaching service of CS Department (http://www-i2.informatik.rwth-aachen.de/Teaching/Service/)

Talks and Publications

Talks

Erika Ábrahám. SAT-Modulo-Theories Solving in the Context of Bounded Model Checking. Invited talk, CWI Amsterdam, Amsterdam, The Netherlands, 2009.

Erika Ábrahám. SMT-solving in the context of bounded model checking. Invited talk, University of Oslo, Oslo, Sweden, 2009.

Erika Ábrahám. On SMT-solving for the Reals. Invited talk, Dagstuhl, Germany, 2009.

Marco Bozzano. The COMPASS Approach: Correctness, Modelling and Performability of Aerospace Systems. Talk, 28th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2009), 2009. Conference Presentation.

Tingting Han. Quantitative model checking of continuous-time Markov chains against timed automata specifications. Talk at VOSS Meeting, University of Twente, NL, 2009.

Tingting Han. Diagnosis, Synthesis and Analysis of Probabilistic Models. Defense Talk, University of Twente, NL, 2009.

Tingting Han. Diagnosis, Synthesis and Analysis of Probabilistic Models. Defense Talk, RWTH Aachen University, Germany, 2009.

Jonathan Heinen. Juggrnaut: Graph Grammar Abstraction for Unbounded Heap Structures. Talk, TTSS 2009, 2009. Workshop Presentation.

Joost-Pieter Katoen. Correctness, Modeling, and Performability of Aerospace Systems: Overview of the COMPASS Project.Talk, COMPASS 2009 Workshop, 2009. Workshop Presentation.

Joost-Pieter Katoen. Abstraction of Probabilistic Systems: From Theory to Practice. Talk at IFIP WG 2.2 Meeting, 2009. Invited presentation.

Joost-Pieter Katoen. The Ins and Outs of the Probabilistic Model Checker MRMC. Talk, QEST 2009, 2009. Conference presentation.

Joost-Pieter Katoen. Verifying Large –and Infinite– Probabilistic Systems. Talk, Fondazione Bruno Kessler, 2009. Departmental Seminar.

Joost-Pieter Katoen. Verifying Infinite Markov Chains. Talk, Nordic Workshop on Programming Theory, Kopenhagen, Denmark, 2009. Invited presentation.

Joost-Pieter Katoen. Model Checking CTMCs Against Linear Real-Time Specifications. Talk, Oxford University, UK, 2009. Departmental Seminar.

Joost-Pieter Katoen. Maximizing Battery Lifetimes by Model Checking. Talk, UMIC Day, RWTH Aachen University, 2009. Invited presentation.

Joost-Pieter Katoen. Verifying CTMCs Against Linear Real-Time Specifications. Talk, Workshop on Quantitative Aspects of Programming Languages, York, UK, 2009. Paper presentation.

Joost-Pieter Katoen. Loop Invariant Generation for Linear Probabilistic Programs. Talk, ROCKS Kick-off Meeting, Vaals, NL, 2009. Presentation.

Joost-Pieter Katoen. Parameter Synthesis for Probabilistic Timed Reachability. Talk, ENS Cachan, Departmental seminar, 2009.

Joost-Pieter Katoen. Achievements in Probabilistic Model Checking. Talk, Quasimodo Review Meeting, Brussels, Belgium, 2009.

Joost-Pieter Katoen. Parameter Synthesis for Probabilistic Timed Reachability. Talk, NICTA Research Center, Sydney, Australia, 2009. Invited presentation.

Joost-Pieter Katoen. Abstraction of Markov Chains. Talk, University of Dortmund, Germany, 2009.

Joost-Pieter Katoen. Abstraction and Refinement of Probabilistic Systems. Talk, Dagstuhl Seminar on Refinement, Wadern, Germany, 2009.

Joost-Pieter Katoen. Parameter Synthesis for Probabilistic Systems. Talk, 2008. Invited talk at opening Modelling of Information Technology Laboratory (MT-LAB), Copenhagen, Denmark.

Joost-Pieter Katoen. Abstraction of Probabilistic Systems: From Theory to Practice. Talk, CDC Workshop on Stochastic Hybrid Systems, Cancun, Mexico, 2008. Keynote Presentation.

Daniel Klink. Time-Bounded Reachability in Tree-Structured QBDs by Abstraction. Talk, AlgoSyn seminar, 2009. Seminar Presentation.

Daniel Klink. Time-Bounded Reachability in Tree-Structured QBDs by Abstraction. Talk, ROCKS, 2009. Workshop Presentation.

Daniel Klink. Compositional abstraction for stochastic systems. Talk, AlgoSyn seminar, 2009. Seminar Presentation.

Daniel Klink. Compositional abstraction for stochastic systems. Talk, FORMATS, 2009. Conference Presentation.

Daniel Klink. Three-valued abstraction for continuous-time Markov chains. Talk, Model Checking @ RWTH, 2008. Workshop Presentation.

Ulrich Loup. Controller Synthesis of Discrete-Continuous Systems using SMT Solving. Gemeinsamer Workshop der Informatik-Graduiertenkollegs und Forschungskollegs, 2009.

Ulrich Loup. Controller Synthesis of Discrete-Continuous Systems using SMT Solving. Seminar talk, 2009.

Alexandru Mereacre. Quantitative Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications.Talk at ULB, Brussels, Belgium, 2009.

Alexandru Mereacre. Quantitative Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications.Talk at AlgoSyn seminar, Aachen, Germany, 2009.

Alexandru Mereacre. Quantitative Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications.Talk at LICS, LA, USA, 2009.

Alexandru Mereacre. Approximate parameter synthesis for probabilistic time-bounded reachability. Talk at Dagstuhl, Germany, 2009.

Alexandru Mereacre. LTL model checking of time-inhomogeneous Markov chains. Talk at TUD, Dortmund, Germany, 2009.

Martin R. Neuhäußer. Delayed Nondeterminism in Continuous-Time Markov Decision Processes. Talk at FoSSaCS 2009, York, England., 2009.

Viet Yen Nguyen. Correctness, Modelling and Performability of Aerospace Systems: Overview of the COMPASS Project. Talk at Charles University in Prague, 2009.

Viet Yen Nguyen. MoonWalker: Verification of .NET Programs. Talk TACAS Workshop 2009, 2009.

Viet Yen Nguyen. Memoised Garbage Collection for Software Model Checking. Talk TACAS Workshop 2009, 2009.

Viet Yen Nguyen. MoonWalker: Verification of .NET Programs. Talk at Charles University in Prague, 2009.

Viet Yen Nguyen. Demo: Perfomability and Model Extension. Talk COMPASS PQR Meeting, 2009.

Viet Yen Nguyen. Codesign of Dependable Systems: A Component-Based Modelling Language. Talk at MEMOCODE 2009 Workshop, 2009.

Viet Yen Nguyen. Correctness, Modelling and Performability of Aerospace Systems. Talk at Marktoberdorf Summer School, 2009.

Viet Yen Nguyen. Verification and Performance Evaluation of AADL Models. Demonstration at ESEC/FSE 2009, Amsterdam, Netherlands, 2009.

Viet Yen Nguyen. Safety, Dependability and Performance Analysis of Extended AADL Models. Talk at ROCKS Kick-Off Meeting, 2009.

Viet Yen Nguyen, and Thomas Noll. System and Software Co-Engineering: Performance and Verification. Talk, ESA Workshop on Avionics Data, Control and Software Systems (ADCSS 2008), 2008. Workshop presentation.

Viet Yen Nguyen. Incremental Hashing for SPIN. Talk, SPIN 2008, 2008. Workshop Presentation.

Viet Yen Nguyen. Architectural Design. Talk, Preliminary Design Review Meeting, Trento, Italy, 2008. Workshop Presentation.

Viet Yen Nguyen. Optimising Techniques for Model Checkers: De noodzaak en uitdaging ervan. Talk, NGI Award Ceremony 2008, 2008. Invited Presentation.

Viet Yen Nguyen. Model Checking .NET Programs. Talk, Model Checking @ RWTH, 2008. Workshop Presentation.

Thomas Noll. A System-Level Integrated Modeling Language for Aerospace Applications. Talk, German Chapter CONCUR Meeting, 2009. Workshop Presentation.

Thomas Noll. A System-Level Integrated Modeling Language for Aerospace Applications. Talk, COMPASS 2009 Workshop, 2009. Workshop Presentation.

Thomas Noll. A System-Level Integrated Modeling Language: Possible Extensions of AADL and Its Error Model Annex. Talk, AADL Standard Meeting, 2009.

Thomas Noll. Correctness, Modeling, and Performability of Aerospace Systems: Formal Semantics of the SLIM Language. Talk, AADL Standard Meeting at Ada-Europe, 2009.

Stefan Rieger. Verification of Pointer Programs. Informatik Oberseminar, RWTH Aachen, , 2009.

Stefan Rieger. Juggernaut: Just Use Graph GRammars to Nicely Abstract Unbounded Structures. DCON 2009, Berlin, , 2008.

Marco Roveri. Symbolic Verification of System-Level Specifications for Aerospace Applications. Talk, COMPASS 2009 Workshop, 2009. Workshop Presentation.

Publications

Niels H.M. Aan de Brugh, Viet Yen Nguyen, and Theo C. Ruys. MoonWalker: Verification of .NET Programs. In Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS. Springer-Verlag, 2009.

Stefan Rieger. Verification of Pointer Programs. PhD Thesis, RWTH Aachen University, 2009.

Erika Ábrahám, Immo Grabe, Andreas Grüner, and Martin Steffen. Behavioral interface description of an object-oriented language with futures and promises. Journal of Logic and Algebraic Programming, 78(7):491–518, 2009.

Erika Ábrahám, Tobias Schubert, Bernd Becker, Martin Fraenzle, and Christian Herde. Parallel SAT Solving in Bounded Model Checking. Journal of Logic and Computation, , 2009.

Erika Ábrahám, Frank S. de Boer, Willem-Paul de Roever, and Martin Steffen. A Deductive Proof System for Multithreaded Java with Exceptions. Fundamenta Informaticae, 82(4):391–463, 2008.

Erika Ábrahám, Andreas Grüner, and Martin Steffen. Heap-Abstraction for an Object-Oriented Calculus with Thread Classes.Software and Systems Modeling, 7(2):177–208, 2008.

Erika Ábrahám, Andreas Grüner, and Martin Steffen. Abstract Interace Behavior of Object-Oriented Languages with Monitors.Theory of Computing Systems, 43(3):322–361, 2008.

Benedikt Bollig, Peter Habermehl, Carsten Kern, and Martin Leucker. Angluin-Style Learning of NFA. In Proceedings of the Twenty-first International Joint Conference on Artificial Intelligence (IJCAI-09). pages 1004–1009. AAAI Press, 2009.

Benedikt Bollig, Peter Habermehl, Carsten Kern, and Martin Leucker. Angluin-Style Learning of NFA. Technical Report LSV-08-28, Laboratoire Spécification et Vérification, ENS Cachan, France, 2008.

Marco Bozzano, Alessandro Cimatti, Marco Roveri, Joost-Pieter Katoen, Viet Yen Nguyen, and Thomas Noll. Codesign of Dependable Systems: A Component-Based Modeling Language. In Proc. 7th ACM-IEEE Int. Conf. on Formal Methods and Models for Codesign (MEMOCODE 2009). ACM Press, 2009.

Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri. The COMPASS Approach: Correctness, Modelling and Performability of Aerospace Systems. In 28th Int. Conf. on Computer Safety, Reliability and Security (SAFECOMP 2009). pages 173–186. Volume 5775 of LNCS. Springer, 2009.

Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri. Verification and Performance Evaluation of AADL Models (Tool Demonstration). In Proc. 7th Joint Meeting of European Software Engineering Conference and ACM SIGSOFT Symp. on the Foundations of Software Engineering (ESEC/FSE 2009). pages 285–286. ACM Press, 2009.

Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri. Model-Based Codesign of Critical Embedded Systems. In Proc. 2nd Int.

Workshop on Model Based Architecting and Construction of Embedded Systems (ACES-MB 2009). LNCS. Springer, 2009.

Manuela Bujorianu, and Joost-Pieter Katoen. Symmetry reduction for stochastic hybrid systems. In Proceedings 47th IEEE Conference on Decision and Control (CDC). pages 233–238. IEEE Control Systems Society, 2008.

Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. Quantitative model checking of continuous-time Markov chains against timed automata specifications. Technical Report AIB-2009-02, RWTH Aachen University, 2009.

Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. Quantitative Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications. In IEEE Symposium on Logic in Computer Science (LICS). IEEE CS Press, 2009.

Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. LTL model checking of time-inhomogeneous Markov chains. In 7th International Symposium on Automated Technology for Verification and Analysis (ATVA'09). pages 104–119. Volume 5799 of LNCS. 2009.

Markus Geimer, Felix Wolf, Brian J. N. Wylie, Erika Ábrahám, Daniel Becker, and Bernd Mohr. The SCALASCA Performance Toolset Architecture. In Proc. of the International Workshop on Scalable Tools for High-End Computing (STHEC'08). pages 56–65. 2008.

Tingting Han, Joost-Pieter Katoen, and Berteun Damman. Counterexample Generation in Probabilistic Model Checking. IEEE Transactions on Software Engineering, 35(2):241–257, 2009.

Tingting Han. Diagnosis, Synthesis and Analysis of Probabilistic Models. PhD Thesis, University of Twente and RWTH Aachen University, 2009.

Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. Approximate parameter synthesis for probabilistic time-bounded reachability. In Proceedings of IEEE Real-Time Systems Symposium (RTSS). pages 173–182. IEEE CS Press, 2008.

Jonathan Heinen, Thomas Noll, and Stefan Rieger. Juggrnaut: Graph Grammar Abstraction for Unbounded Heap Structures. InProc. 3rd Int. Workshop on Harnessing Theories for Tool Support in Software (TTSS'09). To be published in ENTCS. Elsevier, 2009.

Marijn R. Jongerden, Boudewijn R. Haverkort, Henrik Bohnenkamp, and Joost-Pieter Katoen. Maximizing System Lifetime by Battery Scheduling. In Proc. DSN 2009, IEEE Computer Society, 2009.

Natalia Kalinnik, Tobias Schubert, Erika Ábrahám, Ralf Wimmer, and Bernd Becker. Picoso - A Parallel Interval Constraint Solver. In Proc. of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'09). 2009.

Joost-Pieter Katoen, and Ivan S. Zapreev. Simulation-based CTMC Model Checking: An Empirical Evaluation. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

Joost-Pieter Katoen, E. Moritz Hahn, Holger Hermanns, David N. Jansen, and Ivan S. Zapreev. The Ins and Outs of the Probabilistic Model Checker MRMC. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

Joost-Pieter Katoen, Daniel Klink, and Martin R. Neuhäußer. Compositional Abstraction of Stochastic Systems . In Formal Modeling and Analysis of Timed Systems (FORMATS). pages 195–211. Volume 5813 of LNCS. Springer, 2009.

Joost-Pieter Katoen, Daniel Klink, and Martin R. Neuhäußer. Compositional Abstraction for Stochastic Systems. Technical Report AIB-2009-15, RWTH Aachen, 2009.

Carsten Kern. Learning Communicating and Nondeterministic Automata. PhD Thesis, RWTH Aachen University, 2009.

Daniel Klink, Anne Remke, Boudewijn R. Haverkort, and Joost-Pieter Katoen. Time-Bounded Reachability in Tree-Structured QBDs by Abstraction. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

Angelika Mader, Henrik Bohnenkamp, Yaroslav S. Usenko, David N. Jansen, Johann Hurink, and Holger Hermanns. Synthesis and Stochastic Assessment of Cost-Optimal Schedules. Software Tools for Technology Transfer, to appear, 2009.

Ralf Mitsching, Carsten Weise, André Kolbe, Henrik Bohnenkamp, and Norbert Berzen. Towards an industrial strength process for timed testing. In Proc. IEEE ICSTW 2009. pages 29–38. IEEE Computer Society, 2009.

Martin R. Neuhäußer, Marielle Stoelinga, and Joost-Pieter Katoen. Delayed Nondeterminism in Continuous-Time Markov Decision Processes. In Foundations of Software Science and Computation Structures (FoSSaCS). pages 364–379. Volume 5504 of LNCS. Springer-Verlag, 2009.

Viet Yen Nguyen, and Theo C. Ruys. Memoised Garbage Collection for Software Model Checking. In Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). LNCS. Springer-Verlag, 2009.

Bastian Schlich, Thomas Noll, Jörg Brauer, and Lucas Brutschy. Reduction of Interrupt Handler Executions for Model Checking Embedded Software. In Proc. of Haifa Verification Conference 2009 (HVC 2009). LNCS. Springer, 2009.

Felix Wolf, Brian J. N. Wylie, Erika Ábrahám, Daniel Becker, Wolfgang Frings, Karl Fürlinger, Markus Geimer, Marc-Andre Hermanns, Bernd Mohr, Shirley Moore, Matthias Pfeifer, and Zoltan Szebenyi. Usage of the SCALASCA Toolset for Scalable Performance Analysis of Large-Scale Parallel Applications. In Proc. of the 2nd HLRS Parallel Tools Workshop. pages 157–167. 2008.

Lijun Zhang, Friedrich Eisenbrand, Holger Hermanns, and David N. Jansen. Flow Faster: Efficient Decision Algorithms for Probabilistic Simulations. Logical Methods in Computer Science, 4(4), 2008.