RISE worldwide Research Internships in Science and Engineering

DAAD Deutscher Akademischer Austauschdienst German Academic Exchange Service

RISE worldwide 2021

RISE worldwide starts its twelveth year! In the past years almost 2500 German undergraduate students interned abroad as research assistants. And once more **Research groups from all over the world** that are interested in **hosting a German research assistant** in the summer of 2021 are invited to submit project offers to RISE worldwide. Canadian professors already had to submit their offer through the Mitacs database as **Mitacs** handles the Canadian side of the program.

How does RISE worldwide work?

In this program research groups, laboratories and doctoral students can apply to host a motivated and well-qualified student from Germany. The German intern will assist in research and lab work for the proposed project. The students have academic training in the fields of **biology, chemistry, physics, earth sciences, engineering, computer science, medicine or a closely related field** and will receive a DAAD scholarship to help cover living expenses and travel costs.

What are the benefits of the program?

Researchers in science and engineering profit both professionally and personally: They receive assistance with their research projects, strengthen their ties to Germany, and extend their knowledge of the German culture, research landscape and higher education system. PhD students are especially encouraged to participate because they in particular can benefit by learning how to be a mentor to younger students. RISE worldwide offers an excellent opportunity to establish academic partnerships with universities in Germany or to intensify already existing transatlantic networks.

German undergraduate students in science and engineering are exposed to advanced research work while gaining desirable practical experience in their respective fields during the summer. They get the chance to develop intercultural competence and improve their language skills. Moreover, the intensive lab work and leisure time spent together with mentors, colleagues and other interns may establish long-lasting friendships.

Visit our website: **www.daad.de/rise-worldwide**
Contact us directly: **rise-ww@daad.de**

Submission of project proposals:	September 1st, 2020 through October 15th, 2020
Terms of the internship:	6 weeks to 3 months in summer 2021 earliest starting date: June 1st, 2021

Canadian project submission was by June 16, 2020 through Mitacs

Federal Ministry of Education and Research

Formal, machine-checked verification of concurrent OS-code

(Internship @ Data61, CSIRO, Sydney, Australia)

The project

Formal verification is important in safety critical software. To make sure a verified system runs correctly one also needs to provide formal guarantees about the correctness of the underlying operating system (OS) that the program runs on. Data61's Trustworthy Systems group is famous for its formal verification of the seL4 microkernel in the Isabelle-HOL theorem prover.

Most recent successfully verified operating systems, including seL4, run on uniprocessor platforms and with interrupts largely disabled. However, there is an increasing demand for verified real-time operating systems (RTOS) which require support for concurrency.

Our team is aiming at providing frameworks for reasoning about concurrency in OS-code [0]. Our main project is to model and verify a multicore version of seL4.

The seL4 kernel has been embedded in high-assurance autonomous flying vehicles that have been developed in collaboration with industry and university partners.

The verification of multicore seL4 targets the "big lock" version of seL4 [1] and is aiming at providing a formal model of interleaved execution. This also includes investigation of the best logic and concurrency model to use.

The candidate would be embedded in our team. To begin with they would work on investigating and comparing various approaches in terms of their expressiveness, applicability and scalability, and/or on improving the automation, and compositionality of the frameworks. The exact work to be done will be set according to the applicant's interests and strengths.

References

[0] https://ts.data61.csiro.au/projects/concurrency/multicore-sel4.pml

[1] "For a microkernel, a big lock is fine" APSys'15. https://ts.data61.csiro.au/publications/nictaabstracts/8768.pdf

General Information

Data61 is Australia's leading digital research powerhouse, offering the research capabilities, IP and collaboration programs to unleash the country's digital and data-driven potential, with a global context. By driving collaboration across industry, academia, government and the startup space, Data61 is able to help existing industries transform, and act as a catalyst in the creation of new technology-based industries.

The intern will be part of *Concurrency and Protocol Verification* (http://ts.data61.csiro.au/projects/concurrency/home.pml), a highly motivated group with different backgrounds (e.g., formal methods and network engineers), working at different institutes (Data61, UNSW). The successful applicant will work together with Dr. June Andronick, Corey Lewis and the rest of the *Multicore seL4 Verification* team.

Sydney is the largest and most populous city in Australia. It is located on Australia's south-east coast of the Tasman Sea. With an approximate population of 5 million in the Sydney metropolitan area the city is the largest in Oceania. Sydney also ranks among the top 10 most liveable cities in the world according to Mercer Human Resource Consulting and The Economist.

Contact Information

If you have any questions concerning the internship, please do not hesitate to contact Corey Lewis.

CONTACT US

t 1300 363 400
+61 3 9545 2176
e csiroenquiries@csiro.au
w www.data61.csiro.au

AT CSIRO WE SHAPE THE FUTURE

We do this by using science and technology to solve real issues. Our research makes a difference to industry, people and the planet.

FOR FURTHER INFORMATION

Corey Lewis
t +61 2 9490 5858
e Corey.Lewis@data61.csiro.au
w www.data61.csiro.au

Modelling and Verification of Routing Protocols

Research Internship @ ANU, Canberra, Australia

Background

Wireless Mesh Networks (WMNs) are a promising technology that is currently being used in a wide range of application areas, including public safety, transportation, mining, etc. Typically, these networks do not have a central component (router), but each node in the network acts as an independent router, regardless of whether it is connected to another node or not. They allow reconfiguration around broken or blocked paths by “hopping” from node to node until the destination is reached. Unfortunately, the performance of current systems often does not live up to the expectations of end users in terms of performance and reliability, as well as ease of deployment and management.

We explore and develop adaptive network protocols and mechanisms for WMNs that can overcome the major performance and reliability limitations of current systems. To support the development of these new protocols, the project also aims at new Formal Methods based techniques, which can provide powerful new tools for the design and evaluation of protocols and can provide critical assurance about protocol correctness and performance.

Research Questions and Tasks

Routing protocol specifications are usually written in plain English. Often this yields ambiguities, inaccuracies or even contradictions. Moreover no formal guarantees can be given based on such a description. The use of Formal Methods such as process algebra avoids these problems, leading not only to a precise description of protocols, but also allowing formal reasoning. The project’s work will be in this area; it can include

Modelling Routing Protocols So far we have modelled three of the standard protocols using process algebra, namely OLSR and AODV, as well as a draft successor protocol that is currently being discussed by the Internet Engineering Task Force (IETF). The project’s work could include the formalisation of another standard protocol such as HWMP (`http://en.wikipedia.org/wiki/IEEE_802.11s`).

Verifying Routing Protocols Based on a faithful specification that has been given, the work could include the verification of basic properties of the routing protocol: packet delivery for example guarantees that a packet, which is injected into a network, is finally delivered at the destination (if the destination can be reached).

Protocol Comparison Often one reads claims like “Protocol A is better than protocol B”. These claims are usually justified by test-bed evaluation and simulation. However, no formal framework exists to compare protocols on grounds of formal methods. Therefore another direction of the project could be the development of such as framework. This should include the development of formal definitions for measurements for protocol quality.

Tool Support The generation of tools for (semi)automatic reasoning is of high interest. For our work we have used the interactive theorem prover Isabelle and the model checker Uppaal. The project’s work could aim at more automation: this can be automatic translation software from a process algebra language to a language that supports automatic tools; examples are FDR, nuXmv, or CADP. The development of proof-tactics for Isabelle is also an option.

The concrete topic is set according to the applicant’s interests and strengths.

General Information

The Australian National University (ANU) is a research-intensive university with research priorities reflecting the challenges facing the world today. At the ANU College of Engineering and Computer Science, you will be integrated into Australia's leading university – with a community of innovative students, teachers and researchers who are finding solutions to the world's greatest challenges in engineering and computer science. ANU is situated in the centre of Canberra, the capital city of Australia.

The intern will work with A/Prof. Peter Höfner
(`https://cecs.anu.edu.au/people/peter-hoefner`)
(https://cecs.anu.edu.au/people/peter-hoefner) and be integrated into a highly motivated group with different backgrounds (e.g., formal methods and network engineers) working at different institutes including Data61, Australia's digital research powerhouse driving collaboration across industry, government, the startup space and academia, including the University of New South Wales (Sydney), the University of Queensland (Brisbane) and Macquarie University (Sydney). Research visits to other universities will be supported.

Contact Information

If you have any questions concerning the internship, please do not hesitate to contact Peter Höfner.

Australian
National
University

Verifying Liveness Properties in Isabelle/HOL

Research Internship @ ANU, Canberra, Australia

Background

With the growth in complexity of algorithms and designs, the importance of formal verification – proving or disproving a set of correctness properties underlying a system – has been raised. Formal verification of correctness properties becomes even more paramount when concurrent and distributed systems are considered. Correctness properties are usually partitioned into *safety* properties – something bad will not occur – and *liveness* – something good will eventually happen.

While the verification of safety properties is theoretically well established and ready to be deployed at large scale (e.g. [1]), the ensurance of liveness properties is far less understood though it is as crucial as safety when it comes to the analysis of distributed systems. Researchers from the Australian National University (ANU) and from Data61, CSIRO have formulated an assumption called *justness* that is claimed to be exactly right for proving a large class of liveness properties [2]. The idea behind justness is that independent parallel components should not block each other from executing enabled actions. Since justness seems to always hold in real-life implementations, it is considered as a warranted replacement of classical fairness assumptions.

Research Questions and Tasks

To promote justness as *the* fundamental assumption for verifying liveness properties and to provide a scale-able verification framework, the following two problems need to be addressed.

- When verifying liveness properties of a large system, computer scientists often transform the system into a smaller one that behaves semantically equivalent with respect to the properties at hand. To prove that liveness properties are preserved under this transformation, semantic equivalences are used. Unfortunately, classical semantic equivalences, such as bisimilarity, between systems do not accord well with justness [2]. To overcome this deficiency, we currently develop several new semantic equivalences by augmenting each transition of a labelled transition system with the names of the (concurrent) components that are required for that transition.
- For each and every equivalence we prove fundamental properties, such as preservation of justness. As the proofs are often very similar, proof mechanization provides an undeniable advantage: no slip of pen, no oversight, no typos. Moreover, replaying existing proofs in newly developed equivalences speeds up proof development, as it indicates those proof steps that are no longer valid – one can thus concentrate on important changes in the proof.

To support our research, the internship aims at the development of a proof theory in the proof assistant Isabelle/HOL [3] for justness-preserving semantic equivalences.

Prior knowledge of the proof assistant Isabelle/HOL is an advantage, but not a prerequisite; however knowledge in (computational) logic and discrete mathematics is required.

References

[1] P. Gammie, A.L. Hosking & K. Engelhardt (2015): *Relaxing Safely: Verified On-the-fly Garbage Collection for x86-TSO*. In D. Grove & S. Blackburn, editors: Programming Language Design and Implementation (PLDI'15), ACM, pp. 99–109, doi: 10.1145/2737924.2738006.

[2] R.J. van Glabbeek & P. Höfner (2019): *Progress, Justness, and Fairness.* ACM Computing Surveys 52(4), pp. 69:1–69:38, doi: 10.1145/3329125.

[3] T. Nipkow, L.C. Paulson & M. Wenzel (2002): *Isabelle/HOL — A Proof Assistant for Higher-OrderLogic*. Lecture Notes in Computer Science 2283, Springer, doi: 10.1007/3-540-45949-9.

General Information

The Australian National University (ANU) is a research-intensive university with research priorities reflecting the challenges facing the world today. At the ANU College of Engineering and Computer Science, you will be integrated aintoAustralia's leading university – with a community of innovative students, teachers and researchers who are finding solutions to the world's greatest challenges in engineering and computer science. ANU is situated in the centre of Canberra, the capital city of Australia.

The intern will work with PhD student Weiyou Wang and A/Prof. Peter Höfner (`https://cecs.anu.edu.au/people/peter-hoefner`) and integrated in a highly motivated group with different (https://cecs.anu.edu.au/people/peter-hoefner) and be integrated into a highly motivated group with different backgrounds (e.g., formal methods and network engineers) working at different institutes including Data61, Australia's digital research powerhouse driving collaboration across industry, government, the startup space and academia. Research visits to other universities will be supported.

Contact Information

If you have any questions concerning the internship, please do not hesitate to contact Weiyou Wang or Peter Höfner.

CakeML: Formally Verified Functional Programming

(Internship @ Data61, Australia [Canberra or Sydney])

Background

CakeML is a functional programming language (similar to OCaml or Standard ML) with a formal specification (a definition in logic) and a mechanically verified (proven correct) compiler and runtime system. The CakeML compiler is at the forefront of research on verified compilers for functional programming languages, aiming for end-to-end correctness with good performance and reasonable cost. As well as verified compilation to machine code, the CakeML language also supports proof-producing synthesis from programs specified in logic. The CakeML project forms the basis for an approach to building high-assurance computer software using interactive theorem provers.

Research Directions

There are a number of ways to make progress on using interactive theorem provers to build high-assurance software at scale. The project could, for example, be in any of the following areas.

Compiler Optimisations State-of-the-art unverified compilers for functional languages do sophisticated compilation passes to produce efficient code, including, for example, lambda-lifting, inlining, and dead-code elimination. The CakeML compiler includes *verified* implementations of some passes (e.g., multi-argument function introduction, register allocation), however many compilation ideas have yet to receive formal analysis and verification.

Program Verification A verified compiler can be used to compile unverified programs, to avoid bugs introduced by compilation, but really shines in preserving properties of verified programs. There are two existing approaches to producing verified CakeML programs: *proof-producing translation* of algorithms specified in logic, and producing *characteristic formulae* from programs written directly in CakeML. A suitable project could involve combining and extending these approaches, and using them to verify an application.

Formal Semantics CakeML supports a wide range of features for a formally specified language (e.g., modules, user-defined exceptions, arbitrary-precision integers and fixed-width words), but is still quite limited in expressiveness compared to widely-used informally-specified programming languages. Specifying the semantics of a new language feature (e.g., records, nested modules, functors, floating point numbers) would be an interesting basis for a project, which would hopefully also involve extending the compiler and synthesis tools to support the new feature.

The exact topic will be set according to the applicant's interests and strengths. More concrete project possibilities are listed at https://cakeml.org/projects.

General Information

Data61 is Australia's leading digital research powerhouse, offering the research capabilities, IP and collaboration programs to unleash the country's digital and data-driven potential, with a global context. By driving collaboration across industry, academia, government and the startup space, Data61 is able to help existing industries transform, and act as a catalyst in the creation of new technology-based industries.

Contact Information

If you have any questions concerning the internship, please do not hesitate to contact Michael Norrish.

CONTACT US

t 1300 363 400
+61 3 9545 2176
e csiroenquiries@csiro.au
w www.data61.csiro.au

AT CSIRO WE SHAPE THE FUTURE

We do this by using science and technology to solve real issues. Our research makes a difference to industry, people and the planet.

FOR FURTHER INFORMATION

Michael Norrish
t +61 2 6218 3719
e michael.norrish@data61.csiro.au
w ts.data61.csiro.au