DiVerMAS
Distributed Systems Verification with MAS-based Model Checking

Summary

The main focus of the project was the verification of distributed systems using techniques from multi-agent systems (MAS) and epistemic logic. While the original work plan was defined in terms of the modelling language *Creol*, the DiVerMAS project moved its attention to a new version of the language, *ABS*. ABS retains the main features of Creol but comes with an updated syntax to allow, e.g., annotations for adding meta-information to the models. These annotations were used to directly add MAS based specifications and initialisation.

To provide verification techniques to ABS the input language for a MAS-based model checker, ISPL, was used, and a mapping between the two languages was developed. The emphasis in the mapping was on asynchronous message passing between agents, while the infinite state space that is spawned by the infinite data types of ABS was avoided in the initial models by using a finite subset of the language. Based on this subset, an extension of the ABS compiler framework was developed to perform the translation to ISPL, where objects are directly mapped to agents, and the ISPL environment is used for message passing. While the data types were restricted to finite instances, the main features of the language like asynchronous message passing was preserved. The translation was performed using a newly developed module in the ABS compiler framework, which considers the specification of predicates and properties in form of annotations to the model and generates ISPL files that directly can be checked in MCMAS.

While the translation effort was successful and verification showed promising results, initial experiments showed that the performance of the approach was not satisfactory do to the state space explosion of asynchronous communication. To improve the performance, partial order reduction techniques were employed and the data transfer between components was serialised to reduce the number of searched paths and number of actions respectively. A paper describing this approach is currently under review at an international conference.

While the tool implementation showed interesting results, practical verification approaches still require non-exhaustive verification methods like test case generation and simulation. A case study on the example of the AODV algorithm

was published by Dr. Griesmayer together with colleagues from UIO and NR in Oslo. It showed that to apply full formal verification in this domain, further improvements in form of abstraction were necessary. To study abstraction in the context of agent systems and epistemic logic, Dr. Griesmayer collaborated with the VAS group on research and tools that lie in the interest of both DiVerMAS and the FP7 project ACSI. In particular questions about modularity of computation, complex data types and abstraction are in the interest of both projects. Together with Pavel Gonzalez and Alessio Lomuscio he worked on the implementation of GSMC, a model checker for artifact based systems, which organise the control and data flow of business processes during their interaction with external agents. The base system of GSMC was presented at ICWS 2012. The extension to epistemic logic and more detailed agent specifications is currently under review at an international conference and will also be part of an Deliverable for the ACSI project. Currently, Dr. Griesmayer works with the same authors on abstraction techniques for epistemic logic. In particular, the interest lies in three valued abstraction for specifications in the mu calculus. The results, especially the insights about abstraction for epistemic relations, will be applicable to both the ABS model checking approach, and the checker for artifact systems, GSMC.

Contribution to career development

The Marie Curie grant gave Dr. Griesmayer the opportunity to work with colleagues in the areas of multi agent systems, verification of epistemic logic and distributed systems, and by close collaboration with the ACSI project, also gained insights into techniques for artifact based systems. This not only helped in gaining expertise, but also in maintaining and building networks in the scientific community.

This expertise was also one of the main reasons for the successful application as Research Engineer for formal methods with ARM, one of the leading IP designers, which will be Dr. Griesmayer's next position.

Contribution to European excellence and competitiveness

In addition to the results in verification of distributed systems and the collaboration with the ACSI project, the flexibility of the program also allowed Dr. Griesmayer to set up consortia and write proposals for further funding. A travel grant from the Royal Society was successful and allowed, in close collaboration with Dr. Charles Morisset, the application of techniques learned during the DiVerMAS project for refinement and in the area of verification of security policies. A larger, FP7-FET application was organised and submitted together with colleagues from France, Norway, and the UK. Although this application was not successful, the consortium organised by Dr. Griesmayer is continuing its collaboration and will further develop the project idea.