Hongjian Jiang

+49 16092436146 | hongjian.jiang@rptu.de

EDUCATION

Max Planck Institute for Software Systems May 2023 - Apr 2026

Automated Reasoning Doctor

East China Normal University Sep 2019 - Jul 2022

Computer Science Master Software Engineering Shanghai

Yunnan University Sep 2015 - Jul 2019

Computer Science Software Engineering Kunming

Research Paper

Jiang H, Li Y, Tan S, et al. Encoding Induction Proof in Dafny[C]//2021 International Symposium on Theoretical Aspects of Software Engineering (TASE). IEEE, 2021: 95-102.

Zhao Y, **Jiang H**, Lv J, et al. AnB2Murphi: A Translator for ConvertingAlice&Bob Specifications to Murphi [C]. International Conference on Software Engineering and Knowledge Engineering 2021

Liu ZH, **Jiang HJ**, Li YJ, Zhao YX. Automatic verification approach of security protocol based on Alice&Bob language specification. Ruan Jian Xue Bao/Journal of Software, 2021

Hu Z, Wang Z, **Jiang H,** et al. HHML: A Hierarchical Hybrid Modeling Language for Mode based Periodic Controllers[C]. International Conference on Software Engineering and Knowledge Engineering 2021

RESEARCH EXPERIENCE

Endogenous Safety Application Software ConstructionTechnology Sep 2019 - Dec 2020

Shanghai-Beijing

- Background: for current application softwares, formal model and security requirement specification of application software is the basis for security analysis, verification, and correct code implementation.
- Motivation: learn behavior modeling method, communication modeling method, the operational environment, threat and attack modeling method, safety property, and security property.
- Products: propose an integrated development kit for the modeling, verification, and code automatic generation for concurrent application software.

Cache Coherence and Parameterized Protocol Verification Mar 2020 - Jan 2021

Institute of Software, Chinese Academy of Sciences Beijing

- Background: parameterized verification of cache coherence protocols is an important but challenging research problem.
- Motivation: propose a feasible approach to encode induction proof in Dafny which helps programmers to verify the systems.
- Productions: an unified framework to verify the case in cache coherence protocols, loop invariants and security protocols.

Automatic Verification of Security Protocols Nov 2020 - Jun 2021

Institute of Software, Chinese Academy of Sciences Beijing

- Background: the security protocol plays a vital role in 5G and the Internet of Things, verifying the security of security protocol has also received a lot of attention from the industry.
- Motivation: security protocols are often expressed in so-called Alice&Bob notation to describe the messages exchanged between honest principals. And security protocols defined by the A&B specifications can not be applied to the formal verification tool directly.
- Products: propose a novel and general translator which compiles the Alice&Bob specifications of security protocols into the input language of Murphi.

Gigabit AFDX Networking Protocol Verification Sep 2020 - Oct 2021

Shanghai Key Laboratory of Trustworthy Computing Shangha

- Background: abstract redundant frame management, transmission jitter, switch forwarding and frame scheduling mechanism in AFDX protocol, and establish formal model.

- Products: model checker SPIN and UPPAAL are used to model and verify gigabit AFDX network protocols, including redundant frame management model, switch forwarding model, SP scheduling model, FIFO scheduling model, end-to-end transmission delay model and flow control model.

Formal Analysis of Security Protocols Based on Model Checking and Theorem Proving Jul 2021 - Apr 2022

Shanghai Key Laboratory of Trustworthy Computing Shangha Shanghai

- An automatic verification method of security protocol is proposed, which adopts explicit Alice&Bob language specification for modeling security protocols. Based on this method, a set of methodologies and implementation tools for model transformation, analysis and verification are proposed, which can convert Alice&Bob specification model into the Murphi model checking tool for verification.
- A formally verified scheme based on the operation semantics of extended Strand Space theorem is proposed, and the security protocol is modeled and verified in the Murphi model checker.
- A method of Strand Space theorem based on inductive definitions is proposed, which not only provides an inductive specification for bundles, but also provides an efficient and rigorous rule-inductive reasoning technique for bundle properties, and finally implements a mechanized proof through Isabelle/HOL to demonstrate its applicability.

PROFESSIONAL EXPERIENCE

Institute of Software, Chinese Academy of Sciences Mar 2020 - Oct 2021

State Key Laboratory of Computer Science Beijing

Teamwork to validate the parameterized protocol in a specific environment, and propose a unified framework to automatically verify cache coherence protocols in Paraverifier, which solved the NP-hard question.

Oracle (China) Software Systems Co., Ltd. Kunming Branch Dec 2018 - May 2019

Java Engineer java development Kunming , Yunnan

Responsible for the team to collaborate on the research and development of a second-hand commodity trading platform. The website was built through the framework of Spring+SpringMVC+Mybatis, and it was successfully completed.

Zhejiang Huiyou Network Technology Co., Ltd. Jan 2018 - Apr 2018

Java Engineer Back-end department Shaoxing, Zhejiang

Assist the mentor to complete an outsourcing project of corporate maternity and baby products shopping, specifically through the SpringBoot+Mybatis framework to achieve server and front-end page construction, The project went online successfully.

MISCELLANEOUS

- **Skills:** Model Checking, Theorem Proving, Function Programming, Logic and automated reasoning
- **Certifications:** Software Designer
- **Languages:** English
- **Interests:** Basketball、Music、Books
- **Activities:** Student Union President、Volunteers