BAOLUO MENG

(+1) 518-557-9526 ⋄ baoluo.meng@ge.com

RESEARCH INTERESTS

Formal methods, satisfiability modulo theories (SMT), and their applications in the following areas: testing and verification of AI-enabled systems, software systems and blockchain applications, ensuring safety and security of cyber-physical systems, and developing assurance cases towards system certification.

EDUCATION

The University of Iowa, Iowa City, IA, USA *December 2018*
PhD in Computer Science (GPA: 4.03/4.00)

The University of Iowa, Iowa City, IA, USA *May 2014*
Master in Computer Science

Beijing Jiaotong University, Beijing, China *May 2009*
Bachelor of Engineering in Software Engineering

PROFESSIONAL EXPERIENCE

GE Research, Niskayuna, NY
Lead Engineer *April 2020 - present*
Formal Verification Research Engineer *February 2019 - April 2020*

- Contribute to proposals and lead projects funded by DARPA, AFRL and NASA
- Conduct research on applying formal methods and SMT technologies in testing and verification of software systems, blockchain applications and Deep Neural Networks-based systems, ensuring safety and security of cyber-physical systems, and developing assurance cases towards system certification.
- Conduct research, design and development of tools that are used to verify that models and (deep neural networks) systems behave correctly as defined.

GE Research, Niskayuna, NY
Research and Development Intern *Summer 2015, Summer 2016, Summer 2017*

- Develop an in-house tool ASSERT to automatically generate test procedures for system requirements by leverage SMT solvers.
- Research on test cases and procedure generation for requirements involving nonlinear functions.

Pearson, Iowa City, IA
Software Development and Engineering Intern *Summer 2013*

- Design and develop software to test online exam systems for mobile platforms.

The University of Iowa, Iowa City, IA
Research Assistant & Teaching Assistant *August 2012 - December 2018*

- Conduct research and development of tools on satisfiability modulo theories, and formal verification on software.
- Teach classes and hold office hours: Algorithm; Formal Methods in Software Engineering.

PUBLICATIONS

Journal

1. **Baoluo Meng**, William Smith, and Michael Durling, "Security Threat Modeling and Automated Analysis for System Design," SAE Int. J. Transp. Cyber. & Privacy 4(1):2021, https://doi.org/10.4271/11-04-01-0001.
2. **Baoluo Meng**; Larraz, Daniel; Siu, Kit; Moitra, Abha; Interrante, John; Smith, William; Paul, Saswata; Prince, Daniel; Herencia-Zapana, Heber; Arif, M. F.; Yahyazadeh, Moosa; Tekken Valapil, Vidhya; Durling, Michael; Tinelli, Cesare; Chowdhury, Omar. 2021. "VERDICT: A Language and Framework for Engineering Cyber Resilient and Safe System" Systems 9, no. 1: 18. https://doi.org/10.3390/systems9010018
3. Hantao Zhang, **Baoluo Meng**, Yiwen Liang. "Sort Race." Software: Practice and Experience: 2022.

Conference

1. **Baoluo Meng**, Arjun Viswanathan, William Smith, Abha Moitra, Kit Siu, Michael Durling. "Synthesis of Optimal Defenses for System Architecture Design Model in MaxSMT" In NASA Formal Methods Symposium. Springer, Cham, 2022.
2. **Baoluo Meng**, Saswata Paul, Abha Moitra, Kit Siu, Michael Durling. "Automating the Assembly of Security Assurance Case Fragments" In 40th International Conference on Computer Safety, Reliability and Security (SAFECOMP). 2021.
3. Jennifer Barzeele, Kit Siu, **Baoluo Meng** et al. "Experience in Designing for Cyber Resiliency in Embedded DoD Systems" In 31st Annual INCOSE International Symposium on Systems Engineering. 2021.
4. **Baoluo Meng**, Meng Li, Benjamin Beckmann, Yoshifumi Nishida, John Carbone, Dan Yang, Michael Durling. "Towards Developing Trusted Smart Contracts in Simulink". In 1st Workshop on Blockchain and Enterprise Systems (BES). 2020
5. **Baoluo Meng**, Abha Moitra, Andrew Crapo, Saswata Paul, et al. "Towards Developing Formalized Assurance Case". In IEEE/AIAA 34rd Digital Avionics Systems Conference (DASC). IEEE, 2020.
6. Nikita Visnevski, Teresa Hubscher-Younger, Akshay Rajhans, **Baoluo Meng**. "Automatic Synthesis of Information Flow Driven Execution Managers for Embedded Software Applications." In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pp. 1-9. IEEE, 2020.**(Best of Session)**
7. Heber Herencia-Zapana, James Lopez, Glen Gallagher, **Baoluo Meng**, Cameron Patterson, Lakshman Maalolan. "Formal Verification Tool Evaluation For Unmanned Aircraft Containing Complex Functions." In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pp. 1-9. IEEE, 2020.
8. Irfan, Ahmed, Kyle D. Julian, Haoze Wu, Clark Barrett, Mykel J. Kochenderfer, **Baoluo Meng**, and James Lopez. "Towards verification of neural networks for small unmanned aircraft collision avoidance." In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pp. 1-10. IEEE, 2020.
9. James G Lopez, Liling Ren, **Baoluo Meng**, Robert Fisher, Joel Markham, Ryan Spoelhof, Michael Rubenstahl, Scott Edwards, Clark Barrett, "Integration and Flight Test of Small UAS Detect and Avoid on A Miniaturized Avionics Platform". In IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC). IEEE, 2019. **(Best of Session)**

10. Meng Li, **Baoluo Meng**, et al. "Requirements-based Automated Test Generation for Safety Critical Software". In IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC). IEEE, 2019.
11. Kit Siu, Abha Moitra, **Baoluo Meng**, et al. "Architectural and Behavioral Analysis for Cyber Security", In IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)". IEEE, 2019. **(Best of Track & Best of Session)**
12. **Baoluo Meng**, Andrew Reynolds, Cesare Tinelli, and Clark Barrett. "Relational constraint solving in SMT." In International Conference on Automated Deduction, pp. 148-165. Springer, Cham, 2017.
13. Bhattacharyya, Siddhartha, S. Miller, Junxing Yang, Scott Smolka, **Baoluo Meng**, Christoph Sticksel, and Cesare Tinelli. "Verification of quasi-synchronous systems with Uppaal." In 2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), pp. 8A4-1. IEEE, 2014.

Patent

1. Yu, Han, Michael Richard Durling, Kit Yan Siu, Meng Li, **Baoluo Meng**, Scott Alan Stacey, Daniel Edward Russell, and Gregory Reed Sykes. "System and method for test generation from software specification models that contain nonlinear arithmetic constraints over real number ranges." U.S. Patent Application 10/169,217, issued January 1, 2019.

PROJECTS

PrOof Engineering for SYSTEm ARchitecture Design Model (OYSTER) (PI)
Funding Agency: Defense Advanced Research Projects Agency (DARPA)
Time: February 2022 - July 2023
Description: GE Research (GRC), in collaboration with the University of Maryland at Baltimore County (UMBC) and GE Aviation Systems (GEAS), proposes "PrOof Engineering for SYSTEm ARchitecture Design Model (OYSTER)" to develop innovative theories and prototype tools that combine Machine Learning-(ML), Satisfiability Modulo Theories (SMT) and model checking to improve formal proof construction, evolution, and repair for system architecture design model. A summary of OYSTER is given in Figure 1. The team has core technical strength in development and transition of high-assurance tools for industrial use, formal modeling and analysis, model checking, and ML.

RACK Engineering Change Proposal – Secure Assurance Fragment Evidence (Co-PI)
Funding Agency: Defense Advanced Research Projects Agency (DARPA)
Time: January 2022 - March 2022
Description: DARPA recently kicked off the Automated Rapid Certification of Software (ARCOS) program. The goal of ARCOS is to automate the evaluation of software assurance evidence enabling certifiers to determine rapidly that system risk is acceptable. GE is leading the TA 2 Evidence Curation technical area, which will ingest assurance case fragments from the Evidence Generation performers and curate the information in a database that the Assurance Generation performers will query and create validated assurance cases with confidence scores. On the existing contract award, the GE team plans to include data provenance for all the evidence under curation in a secure database. In order to make the evidence more secure, GE and Guardtime Federal (GTF) propose this Engineering Change Proposal effort to explore application of KSI Distributed Cryptography (similar to blockchain) technology to capture and manage development and certification of artifacts. KSI Distributed Cryptography enables the participation of digital artifacts of the state of a file (or files) in a recurring set of cryptographic calculations such that verification of authenticity, authorship, and time of state changes can be immutably verified. Applying KSI data integrity to the evidence itself will ensure that the implementation and certification artifacts have not been

tampered with over the life cycle of the system.

Evaluation of Verification & Validation Tools in a Ummaned Aircraft System Runtime Safety Assurance System (Co-PI)
Funding Agency: National Aeronautics and Space Administration (NASA)
Time: January 2020 - December 2022
Description: GE is developing an embedded avionics system for hosting flight safety critical functions for unmanned aerial systems (UAS). In order to ensure safe operation of UAS in the national airspce, we include a runtime safety assurance (RTSA) system. In year 1, the goal of this project is to evaluate Validation & Verification (V&V) tools on the RTSA system. We will start by detailing and base-lining a traditional V&V process of the RTSA system, capturing metrics at each step of the process. Then we will perform the same V&V process for the RTSA system but will use formal methods based tools at appropriate steps in the process. We will use formal tools such as FRET, AdvoCATE, AGREE, CoCoSim, and ASSERT developed by NASA, DARPA, Virginia Tech and GE. At the end, we will perform a comparison of the two approaches. In year 2, we evaluate the usability and effectiveness of the Adaptive Stress Testing (AST) tool (AdaStress) in an industrial setting, and clarify the role for AST artifacts to support software certification. To achieve this, we will work on integrating NASA Adaptive Stress Testing (AST) tool with GE next-gen product testing tool – Continuum to detect rare failure events in trajectory prediction done by GE Aviation's Flight Management System (FMS).

VERDICT: Verification Evidence & Resilient Design in anticipation of Cybersecurity Threats
Funding Agency: Defense Advanced Research Projects Agency (DARPA)
Time: February 2018 - December 2021
Description: The goal of this project is to develop the necessary design, analysis and verification tools to allow system engineers to design-in cyber resiliency and manage tradeoffs as they do other nonfunctional properties when designing complex embedded computing systems. Cyber resiliency means the system is tolerant to cyberattacks in the same way that safety critical systems are tolerant to random faults—they recover and continue to execute their mission function. Achieving this goal requires research breakthroughs in:

- the elicitation of cyber resiliency requirements before the system is built
- the design and verification of systems when requirements are not testable (i.e., when they are expressed in shall not statements)
- tools to automatically adapt software to new non-functional requirements; and
- techniques to scale and provide meaningful feedback from analysis tools that reside low in the development tool chain

Robustness Verification of Deep Neural Networks (DNNs) Representation of Airborne Collision Avoidance System for small Unmanned Systems (ACAS sXu)
Funding Agency: GE Aviation
Time: February 2019 - August 2020
Description: The Airborne Collision Avoidance System X family has been adopted for manned (ACAS Xa), unmanned aircraft (ACAS Xu) and small unmanned aircraft (ACAS sXu) to reduce the risk of mid-air collisions or near mid-air collision. Traditionally, the decision-making logic of ACAS X is created using a large numeric lookup table (LUT) requiring hundreds of GB storage, which makes it difficult for certification. In this project, we will use a new storage-efficient approach to represent ACAS sXu, which leverages the deep neural network (DNN) to learn a robust nonlinear

function approximation of the lookup table. We will leverage the SMT solver – Marabou to verify the DNNs of ACAS sXu behave smoothly, i.e., small input perturbations should not cause major spikes in the network's output. We hope to form a formal proof that the entire network always behaves as intended.

ASSERT: Analysis of Semantic Specifications and Efficient generation of Requirements -based Tests

Funding Agency: GE Aviation
Time: Summer 2015, Summer 2016, Summer 2017
Description: The size and complexity associated with software that monitors, controls, and protects flight critical products continues to grow. Thus, maintenance, verification and validation of those software requires significant amount of money, time and manpower. To reduce the cost and time associated with the process, we propose a new tool suite for requirements capture and analysis, and test case and test procedure generation for requirements. We introduce a Requirements Capture language developed for use by a requirements engineer that is as close as possible to English, allowing her to write requirements using terms and concepts from her domain, yet is formal enough that requirements written in this language can be analyzed using formal methods. After the requirements analysis, we obtain a set of unambiguous, conflict-free, and complete requirements. Then we will generate test cases and test procedures by leveraging SMT technology to validate that the software implementation satisfies requirements.

CVC4: An efficient open-source automatic theorem prover for satisfiability modulo theories (SMT) problems

Website: https://cvc4.github.io
Funding Agency: https://cvc4.github.io/acknowledgements.html
Time: 2017 – 2018
Description: CVC4 is the state-of-the-art and efficient open-source automatic theorem prover for satisfiability modulo theories (SMT) problems. It can be used to prove the validity (or, dually, the satisfiability) of first-order formulas in a large number of built-in logical theories and their combination. In this project, I design, implement and test a finite sets/relations theory solver. Combining this new solver with the finite model finding features of CVC4 enables several compelling use cases. For instance, native support for relations enables a natural mapping from Alloy, a declarative modeling language based on first-order relational logic, to SMT constraints. It also enables a natural encoding of several description logics with concrete domains, allowing the use of an SMT solver to analyze, for instance, Web Ontology Language (OWL) models.

Formal Analysis and Verification of Unmanned System Autonomy Services (UxAS) Architecture

Funding Agency: United States Air Force Research Lab (AFRL)
Time: 2017 Summer
Description: Software architecture plays an important role in the software development, because system characteristics such as functional correctness, robustness and maintainability depend on the architecture. However, it is not easy to verify if the final software product complies with the original software architecture specifications, especially in the absence of a formally described and documented architecture design, and lack of a formal verification framework to verify the implementation against the original specification. Based on previous experience of extracting design information from legacy software, we use a similar and extended methodology to support formal capture of software architecture models captured in SADL and scalable analysis and verification of UxAS architecture by using an SMT solver – CVC4.

CoCoSim: Automated analysis and compilation framework for Simulink/Stateflow
Website: https://github.com/coco-team/cocoSim2
Funding Agency: National Aeronautics and Space Administration (NASA)
Description: CoCoSim is an automated analysis and code generation framework for Simulink and Stateflow models. Specifically, CoCoSim can be used to verify automatically user-supplied safety requirements. In this project, we develop a translator from the intermediate representation (JSON) of CoCoSim models to Lustre programs, and leverage the Kind2 model checker to verify if CoCoSim models satisfies their contracts.

PROFESSIONAL SERVICE

Artifact Evaluation Committee Member, 23rd International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI), 2022

Session Chair, Reviewer for 40th AIAA Digital Avionics System Conference, 2021

Session Chair, Reviewer for 39th AIAA Digital Avionics System Conference, 2020

AWARDS

Control & Optimization Rookie of the Year, GE Research, Niskayuna NY, 2019

Excellent Beijing Olympic Games Volunteer Leader, Beijing, 2008

MENTORING

- Soumyabrata Talukder, PhD Student, Iowa State University, 2019 Summer
- William Smith, Undergraduate, Cornell University, 2019 Summer, 2020 Summer
- Saswata Paul, PhD Student, Rensselaer Polytechnic Institute, 2020 Summer, 2021 Summer
- Arjun Viswanathan, PhD Student, The University of Iowa, 2021 Summer
- Joyanta Debnath, PhD Student, The University of Iowa, 2021 Summer
- Emmanuel Manolios, Master Student, The University of Northeastern, 2022 Spring

PERSONAL TRAITS

Highly motivated and eager to learn new things.

Strong motivational and leadership skills.

Ability to work as an individual as well as in group.