Wenchao Li

CONTACT INFORMATION

336 PHO
8 Saint Mary's St.
Boston, MA 02215

(617) 353-0115
wenchao@bu.edu
Dependable Computing Lab

RESEARCH INTERESTS

I am a computer scientist working at the intersection of formal methods and machine learning with the goal of building **safe and trustworthy autonomous systems**. My research group at BU develops new theories and tools across several areas including design automation, cyber-physical systems, formal verification, and deep learning.

EMPLOYMENT

Boston University, Boston, Massachusetts, USA.

Assistant Professor, Department of Electrical and Computer Engineering July 2016 – Present

Affiliations: Division of Systems Engineering, Department of Computer Science, Center for Information & Systems Engineering, Hariri Institute for Computing

SRI International, Menlo Park, California, USA.

Computer Scientist March 2015 – June 2016

Postdoctoral Fellow November 2013 – March 2015

EDUCATION

University of California, Berkeley, California, USA.

Ph.D. in Electrical Engineering and Computer Sciences 2007 – 2013

- Dissertation: *Specification Mining: New Formalisms, Algorithms and Applications*
- Advisor: Sanjit A. Seshia
- **ACM Outstanding Ph.D. Dissertation Award in Electronic Design Automation**

University of California, Berkeley, California, USA.

M.S. in Electrical Engineering and Computer Sciences

- Thesis: *Formal Methods for Reverse Engineering Gate-Level Netlists*

University of California, Berkeley, California, USA.

B.S. in Electrical Engineering and Computer Sciences 2003 – 2007

B.A. in Economics 2003 – 2007

HONORS AND AWARDS

Nominated for the Design Automation Conference Under-40 Innovators Award	2023
Nominated for the IEEE Technical Committee on Cyber-Physical Systems Early-Career Award	2019
Peter J. Levine Career Development Professorship, Boston University	2018
Junior Fellow, Hariri Institute for Computing	2018
Hariri Institute Research Incubation Award	2018
ACM SIGDA Outstanding Ph.D. Dissertation Award	2015
Leon O. Chua Award for Outstanding Achievement in Nonlinear Science, UC Berkeley	2013
Best Presentation Award, International Symposium on Hardware-Oriented Security and Trust	2013
Finalist, Best Paper Award, International Symposium on Hardware-Oriented Security and Trust	2012
Finalist, Qualcomm Innovation Fellowship	2012
EECS Outstanding Graduate Student Instructor Honorable Mention, UC Berkeley	2009
University Outstanding Graduate Student Instructor Award, UC Berkeley	2009
Vodafone-US Foundation Fellows Initiative Scholarship	2007

Honors Awarded to My Advisees:

- H M Sabbir Ahmad: Best Student Paper, IEEE Conference on Control Technology and Applications (CCTA) 2023
- Jiameng Fan: Second Place, ACM SIGBED Student Research Competition 2021

Peer-Reviewed Publications

Google Scholar Profile
Citations: 2439; H-Index: 27 (as of July 15, 2023)

We regularly publish at top venues across several areas. *Machine Learning and Artificial Intelligence:* International Conference on Machine Learning (**ICML**), International Conference on Learning Representations (**ICLR**), AAAI Conference on Artificial Intelligence (**AAAI**). *Formal Methods:* International Conference on Computer Aided Verification (**CAV**). *Design Automation:* ACM/EDAC/IEEE Design Automation Conference (**DAC**), International Conference on Computer Aided Design (**ICCAD**), Conference on Design, Automation and Test in Europe (**DATE**). *Embedded and Cyber-Physical Systems:* ACM SIGBED International Conference on Embedded Software (**EMSOFT**). *Multi-Agent Systems:* International Conference on Autonomous Agents and Multiagent Systems (**AAMAS**).

The names of the students advised by me are underlined.

Book Chapters and Ph.D. Thesis

1. Xin Chen, Jiameng Fan, Chao Huang, Ruochen Jiao, **Wenchao Li**, Xiangguo Liu, Yixuan Wang, Zhilu Wang, Weichao Zhou, and Qi Zhu.
   Safety-Assured Design and Adaptation of Connected and Autonomous Vehicles,
   Chapter in Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems, Springer, 2023.
2. **Wenchao Li**.
   Specification Mining: New Formalisms, Algorithms and Applications,
   Ph.D. Thesis, University of California, Berkeley, December 2013.
   Winner of the 2015 ACM Outstanding Ph.D. Dissertation Award in Electronic Design Automation.

Journal Publications

3. Zhilu Wang, Chao Huang, Hyoseung Kim, **Wenchao Li** and Qi Zhu.
   Cross-Layer Adaptation with Safety-Assured Proactive Task Job Skipping,
   ACM Transactions on Embedded Computing Systems (TECS), 20(5s):Article 100, October 2021.
   Also appeared at the ACM SIGBED International Conference on Embedded Software (EMSOFT), 2021.
4. Chao Huang, Jiameng Fan, Xin Chen, **Wenchao Li** and Qi Zhu.
   Divide and Slide: Layer-Wise Refinement for Output Range Analysis of Deep Neural Networks,
   IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 39(11):3323–3335, November 2020.
   Also appeared at the ACM SIGBED International Conference on Embedded Software (EMSOFT), 2020.
5. Chao Huang, Jiameng Fan, **Wenchao Li**, Xin Chen and Qi Zhu.
   ReachNN: Reachability Analysis of Neural-Network Controlled Systems,
   ACM Transactions on Embedded Computing Systems (TECS), 18(5s):Article 106, October 2019.
   Also appeared at the ACM SIGBED International Conference on Embedded Software (EMSOFT), 2019.
6. Sanjit A. Seshia, Shiyan Hu, **Wenchao Li** and Qi Zhu.
   Design Automation of Cyber-Physical Systems: Challenges, Advances, and Opportunities,
   IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 36(9):1421–1434, September 2017. (*Keynote*)
7. Pramod Subramanyan, Nestan Tsiskaridze, **Wenchao Li**, Adrià Gascón, Wei Yang Tan, Ashish Tiwari, Natarajan Shankar, Sanjit A. Seshia and Sharad Malik.
   Reverse Engineering Digital Circuits Using Structural and Functional Analyses,
   IEEE Transactions on Emerging Topics in Computing (TETC), 2(1):63–80, December 2013.

Refereed Conference Publications

8. H M Sabbir Ahmad, Ehsan Sabouni, Wei Xiao, Christos G. Cassandras and **Wenchao Li**.
Trust-Aware Resilient Control and Coordination of Connected and Automated Vehicles,
The 26th IEEE International Conference on Intelligent Transportation Systems (ITSC), September 2023 (to appear). (Acceptance rate unknown)
9. Ehsan Sabouni, H M Sabbir Ahmad, Wei Xiao, Christos G. Cassandras and **Wenchao Li**.
Merging Control in Mixed Traffic with Safety Guarantees: A Safe Sequencing Policy with Optimal Motion Control,
The 26th IEEE International Conference on Intelligent Transportation Systems (ITSC), September 2023 (to appear). (Acceptance rate unknown)
10. H M Sabbir Ahmad, Ehsan Sabouni, Wei Xiao, Christos G. Cassandras and **Wenchao Li**.
Optimal Control of Connected Automated Vehicles with Event-Triggered Control Barrier Functions: a Test Bed for Safe Optimal Merging,
The 7th IEEE Conference on Control Technology and Applications (CCTA), July 2023. (**Best Student Paper Award**) (The first two authors contributed equally to this paper. Acceptance rate unknown)
11. H M Sabbir Ahmad, Ehsan Sabouni, Wei Xiao, Christos G. Cassandras and **Wenchao Li**.
Evaluations of Cyber Attacks on Cooperative Control of Connected and Autonomous Vehicles at Bottleneck Points,
Inaugural ISOC Symposium on Vehicle Security and Privacy (VehicleSec), February 2023 (full paper). (Acceptance rate for full paper: 40.8%)
12. Kacper Wardega, Max von Hippel, Roberto Tron, Cristina Nita-Rotaru and **Wenchao Li**.
Byzantine Resilience at Swarm Scale: A Decentralized Blocklist from Inter-robot Accusations,
The 22nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2023 (full paper). (Acceptance rate: 23.3% for full papers and 45.1% for full papers + extended abstracts)
13. Kacper Wardega, Max von Hippel, Roberto Tron, Cristina Nita-Rotaru and **Wenchao Li**.
HoLA Robots: Mitigating Plan-Deviation Attacks in Multi-Robot Systems with Co-Observations and Horizon-Limiting Announcements,
The 22nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2023 (extended abstract). (Acceptance rate: 23.3% for full papers and 45.1% for full papers + extended abstracts)
14. Chao Huang, Jiameng Fan, Xin Chen, **Wenchao Li** and Qi Zhu.
POLAR: A Polynomial Arithmetic Framework for Verifying Neural-Network Controlled Systems,
The 20th International Symposium on Automated Technology for Verification and Analysis (ATVA), October 2022. (Acceptance rate: 32.1%)
15. Jiameng Fan and **Wenchao Li**.
DRIBO: Robust Deep Reinforcement Learning via Multi-View Information Bottleneck,
The 39th International Conference on Machine Learning (ICML), July 2022. (Acceptance rate: 21.9%)
16. Weichao Zhou and **Wenchao Li**.
A Hierarchical Bayesian Approach to Inverse Reinforcement Learning with Symbolic Reward Machines,
The 39th International Conference on Machine Learning (ICML), July 2022. (Acceptance rate: 21.9%)
17. Feisi Fu and **Wenchao Li**.
Sound and Complete Neural Network Repair with Minimality and Locality Guarantees,
The 10th International Conference on Learning Representations (ICLR), April 2022. (Acceptance rate: 32.3%)
18. Weichao Zhou and **Wenchao Li**.
Programmatic Reward Design by Example,

The 36th AAAI Conference on Artificial Intelligence (AAAI), February 2022. (Acceptance rate: 15.0%)

19. Kacper Wardega, **Wenchao Li**, Hyoseung Kim, Yawen Wu, Zhenge Jia and Jingtong Hu.
Opportunistic Communication with Latency Guarantees for Intermittently-Powered Devices,
Design, Automation and Test in Europe Conference (DATE), March 2022. (Acceptance rate: 25%)

20. Panagiota Kiourti, **Wenchao Li**, Anirban Roy, Karan Sikka and Susmit Jha.
MISA: Online Defense of Trojaned Models using Misattributions,
Annual Computer Security Applications Conference (ACSAC), December 2021. (Acceptance rate: 24.5%)

21. Jiameng Fan and **Wenchao Li**.
Adversarial Training and Provable Robustness: A Tale of Two Objectives,
In Proceedings of the 35th AAAI Conference on Artificial Intelligence (AAAI), February 2021. (Acceptance rate: 21.4%)

22. Qi Zhu, **Wenchao Li**, Hyoseung Kim, Yecheng Xiang, Kacper Wardega, Zhilu Wang, Yixuan Wang, Hengyi Liang, Chao Huang, Jiameng Fan, Hyunjong Choi.
Know the Unknowns: Addressing Disturbances and Uncertainties in Autonomous Systems,
In Proceedings of the 39th International Conference on Computer Aided Design (ICCAD), November 2020. (*Invited*)

23. Weichao Zhou, Ruihan Gao, BaekGyu Kim, Eunsuk Kang and **Wenchao Li**.
Runtime-Safety-Guided Policy Repair,
In Proceedings of the 20th International Conference on Runtime Verification (RV), October 2020. (Acceptance rate unknown)

24. Jiameng Fan, Chao Huang, Xin Chen, **Wenchao Li** and Qi Zhu.
ReachNN: A Tool for Reachability Analysis of Neural-Network Controlled Systems,*
In Proceedings of the 18th International Symposium on Automated Technology for Verification and Analysis (ATVA), October 2020. (Acceptance rate unknown; average Acceptance rate in 2018 and 2019 was 34.9%)

25. Panagiota Kiourti, Kacper Wardega, Susmit Jha and **Wenchao Li**.
TrojDRL: Evaluation of Backdoor Attacks on Deep Reinforcement Learning,
In Proceedings of the 57th ACM/EDAC/IEEE Design Automation Conference (DAC), July 2020. (Acceptance rate: 23%)

26. Chao Huang, Shichao Xu, Zhilu Wang, Shuyue Lan, **Wenchao Li** and Qi Zhu.
Opportunistic Intermittent Control with Safety Guarantees for Autonomous Systems,
In Proceedings of the 57th ACM/EDAC/IEEE ACM/IEEE Design Automation Conference (DAC), July 2020. (Acceptance rate: 23%)

27. Kacper Wardega and **Wenchao Li**.
Application-Aware Scheduling of Networked Applications over the Low-Power Wireless Bus,
In Proceedings of the Conference on Design, Automation and Test in Europe (DATE), March 2020. (Acceptance rate: 26%)

28. Jiameng Fan, Chao Huang, **Wenchao Li**, Xin Chen and Qi Zhu.
Towards Verification-Aware Knowledge Distillation for Neural-Network Controlled Systems,
In Proceedings of the 38th ACM/IEEE International Conference on Computer Aided Design (ICCAD), November 2019. (*Invited*)

29. Kacper Wardega, Roberto Tron and **Wenchao Li**.
Masquerade Attack Detection Through Observation Planning for Multi-Robot Systems,
In Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2019 (extended abstract). (Acceptance rate: 24.2% for full papers and 52.1% for full papers + extended abstracts)

30. Chao Huang, **Wenchao Li** and Qi Zhu.
Formal Verification of Weakly-Hard Systems,
In Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC), April 2019. (Acceptance rate: 25%)

31. Weichao Zhou and **Wenchao Li**.
Safety-Aware Apprenticeship Learning,
In Proceedings of the 30th International Conference on Computer Aided Verification (CAV), July 2018. (Acceptance rate: 27%)

32. Qi Zhu, Hengyi Liang, Licong Zhang, Debayan Roy, **Wenchao Li**and Samarjit Chakraborty.
Extensibility-Driven Automotive In-Vehicle Architecture Design,
In Proceedings of the 54th ACM/EDAC/IEEE Design Automation Conference (DAC), June 2017. (*Invited*)

33. Bowen Zheng, Chung-Wei Lin, Hengyi Liang, Shinichi Shiraishi, **Wenchao Li** and Qi Zhu.
Delay-Aware Design, Analysis and Verification of Intelligent Intersection Management,
In Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP), May 2017. (Acceptance rate unknown)

34. Xiaodao Chen, Yuchen Zhou, Hong Zhou, Chaowei Wan, Qi Zhu, **Wenchao Li** and Shiyan Hu.
Analysis of Production Data Manipulation Attacks in Petroleum Cyber-Physical Systems,
In Proceedings of the 35th IEEE/ACM International Conference on Computer-Aided Design (ICCAD), November 2016. (*Invited*)

35. Devesh Bhatt, Arunabh Chattopadhyay, **Wenchao Li**, David Oglesby, Sam Owre and Natarajan Shankar.
Contract-Based Verification of Complex Time-Dependent Behaviors in Avionic Systems,
In Proceedings of the 8th NASA Formal Methods Symposium (NFM), June 2016.

36. Shalini Ghosh, Daniel Elenius, **Wenchao Li**, Patrick Lincoln, Natarajan Shankar and Wilfried Steiner.
ARSENAL: Automatic Requirements Specification Extraction from Natural Language,
In Proceedings of the 8th INASA Formal Methods Symposium (NFM), June 2016.

37. **Wenchao Li**, Hassen Saïdi, Huascar Sanchez, Martin Schäf and Pascal Schweitzer
Detecting Similar Programs via the Weisfeiler-Leman Graph Kernel,
In Proceedings of the 15th International Conference on Software Reuse (ICSR), June 2016.

38. **Wenchao Li**, Léonard Gérard and Natarajan Shankar.
Design and Verification for Multi-Rate Distributed Systems,
In Proceedings of the 13th ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE), September 2015.

39. Bowen Zheng, **Wenchao Li**, Peng Deng, Léonard Gérard, Qi Zhu and Natarajan Shankar.
Design and Verification for Transportation System Security,
In Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), June 2015. (*Invited*)

40. **Wenchao Li**, Dorsa Sadigh, S. Shankar Sastry and Sanjit A. Seshia.
Synthesis for Human-in-the-Loop Control Systems,
In Proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), April 2014.

41. Alberto Puggelli, **Wenchao Li**, Alberto Sangiovanni-Vincentelli and Sanjit A. Seshia.
Polynomial-Time Verification of PCTL Properties of MDPs with Convex Uncertainties,
In Proceedings of the 25th International Conference on Computer Aided Verification (CAV), July 2013.

42. **Wenchao Li**, Adrià Gascón, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar and Sanjit A. Seshia.
WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates,
In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), June 2013. (**Best Presentation Award**)

43. **Wenchao Li** and Sanjit A. Seshia.
Sparse Coding for Specification Mining and Error Localization,
In Proceedings of the International Conference on Runtime Verification (RV), September 2012.

44. **Wenchao Li**, Zach Wasson and Sanjit A. Seshia.
Reverse Engineering Circuits Using Behavioral Pattern Mining,
In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), June 2012. (**Best Paper Finalist**)

45. **Wenchao Li**, Sanjit A. Seshia and Somesh Jha.
CrowdMine: Towards Crowdsourced Human-Assisted Verification,
In Proceedings of the 49th ACM/EDAC/IEEE Design Automation Conference (DAC), June 2012.

46. **Wenchao Li**, Lili Dworkin and Sanjit A. Seshia.
Mining Assumptions for Synthesis,
In Proceedings of the 9th ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE), July 2011.

47. **Wenchao Li**, Alessandro Forin and Sanjit A. Seshia.
Scalable Specification Mining for Verification and Diagnosis,
In Proceedings of the 47th ACM/EDAC/IEEE Design Automation Conference (DAC), June 2010.

48. **Wenchao Li**, Marco D. Natale, Wei Zheng, Paolo Giusto, Alberto Sangiovanni-Vincentelli and Sanjit A. Seshia.
Optimizations of an Application-Level Protocol for Enhanced Dependability in FlexRay,
In Proceedings of the Conference on Design, Automation and Test in Europe (DATE), April 2009.

49. Daniel Holcomb, **Wenchao Li** and Sanjit A. Seshia.
Design as You See FIT: System-Level Soft Error Analysis of Sequential Circuits,
In Proceedings of the Conference on Design, Automation and Test in Europe (DATE), April 2009.

50. Orna Kupferman, **Wenchao Li** and Sanjit A. Seshia.
A Theory of Mutations with Applications to Vacuity, Coverage, and Fault Tolerance,
In Proceedings of the IEEE International Conference on Formal Methods in Computer-Aided Design (FMCAD), November 2008.

51. Sanjit A. Seshia, **Wenchao Li** and Subhasish Mitra.
Verification-Guided Soft Error Resilience,
In Proceedings of the Conference on Design, Automation and Test in Europe (DATE), April 2007.

52. Roozbeh Jafari, **Wenchao Li**, Ruzena Bajcsy, Steven Glaser and Shankar Sastry.
Physical Activity Monitoring for Assisted Living at Home,
In Proceedings of the 4th International Conference on Wearable and Implantable Body Sensor Networks (BSN), March 2007.

Refereed Workshop Papers

53. Feisi Fu, Zhilu Wang, Jiameng Fan, Yixuan Wang, Chao Huang, Xin Chen, Qi Zhu, **Wenchao Li**.
REGLO: Provable Neural Network Repair for Global Robustness Properties,
Conference on Neural Information Processing Systems (NeurIPS), Workshop on Trustworthy and Socially Responsible Machine Learning (TSRML), December 2022.

54. Kacper Wardega, Roberto Tron and **Wenchao Li**.
Resilience of Multi-Robot Systems to Physical Masquerade Attacks,
In Proceedings of the IEEE Workshop on the Internet of Safe Things (SafeThings), May 2019.

55. Jiameng Fan and **Wenchao Li**.
Safety-Guided Deep Reinforcement Learning via Online Gaussian Process Estimation,
International Conference on Learning Representation (ICLR), Workshop on Safe Machine Learning: Specification, Robustness, and Assurance, May 2019.

56. Chao Huang, Kacper Wardega, **Wenchao Li** and Qi Zhu.
Exploring Weakly-hard Paradigm for Networked Systems,
In Proceedings of the 1st Workshop on Design Automation for CPS and IoT (DESTION), April 2019.

57. Dorsa Sadigh, Katherine Driggs-Campbell, Alberto Puggelli, **Wenchao Li**, Victor Shia, Ruzena Bajcsy, Alberto Sangiovanni-Vincentelli, S. Shankar Sastry and Sanjit A. Seshia.
Data-Driven Probabilistic Modeling and Verification of Human Driver Behavior,
Formal Verification and Modeling in Human-Machine Systems, AAAI Spring Symposium, March 2014.

58. **Wenchao Li**, Susmit Jha and Sanjit A. Seshia.
Power-Aware Dynamic Control of Error-Resilience Mechanisms,
The 9th Workshop on Silicon Errors in Logic – System Effects (SELSE), March 2013.

59. Susmit Jha, **Wenchao Li** and Sanjit A. Seshia.
Localizing Transient Faults Using Dynamic Bayesian Networks,
IEEE International High Level Design Validation and Test Workshop (HLDVT), November 2009.

Technical Reports

60. Diego Manzanas Lopez, Matthias Althoff, Luis Benet, Xin Chen, Jiameng Fan, Marcelo Forets, Chao Huang, Taylor T. Johnson, Tobias Ladner, **Wenchao Li**, Christian Schilling and Qi Zhu.
ARCH-COMP22 Category Report: Artificial Intelligence and Neural Network Control Systems (AINNCS) for Continuous and Hybrid Systems Plants,
Proceedings of 9th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH22), vol. 90, pages 142–184.

61. Daniel Holcomb, **Wenchao Li** and Sanjit A. Seshia.
Algorithms for Green Buildings: Learning-Based Techniques for Energy Prediction and Fault Diagnosis,
Technical Report, University of California, Berkeley, UCB/EECS-2009-138, October 2009.

62. Orna Kupferman, **Wenchao Li** and Sanjit A. Seshia.
On the Duality between Vacuity and Coverage,
Technical Report, University of California, Berkeley, UCB/EECS-2008-26, March 2008.

Software Release

DBP, implementation of a decentralized blocklist protocol for Byzantine resilience in multi-robot systems, https://github.com/BU-DEPEND-Lab/DBP

DRIBO, a tool for performing robust deep reinforcement learning on inputs with visual distractions, https://github.com/BU-DEPEND-Lab/DRIBO

POLAR, a tool for performing reachability analysis of neural-network controlled systems using Taylor model approximations, https://github.com/BU-DEPEND-Lab/POLAR

*ReachNN**, a tool for performing reachability analysis of neural-network controlled systems using Bernstein polynomial approximations (subsumed by POLAR), https://github.com/BU-DEPEND-Lab/ReachNNStar

REASSURE, a tool for performing neural network repairs, https://github.com/BU-DEPEND-Lab/REASSURE

AdvIBP, a tool for adversarial training of deep neural networks with provable robustness guarantees, https://github.com/BU-DEPEND-Lab/AdvIBP

TrojDRL, a tool for evaluating backdoor attacks in deep reinforcement learning, https://github.com/BU-DEPEND-Lab/TrojDRL

Funding

Total External Funding (Personal Share Only): >$2.3 million

Robust AI – Robustness Analysis of Prompts, **Intuit**, Sole PI, $75,000, 2023 – 2024.

Robust AI – A Unified and Robust Attribution Analysis Framework for Interpretable Deep Learning, **Intuit**, Sole PI, $75,000, 2022 – 2023.

Trojan Detection using Attribution, Counterfactuals, and Topological Analysis (DECANT), **IARPA**, BU PI (Team: SRI International + BU + Stony Brook University), $850,000 (total: ∼$7,000,000), 8/2020 – 10/2024.

CPS: Medium: Collaborative Research: Multiagent Physical Cognition and Control Synthesis Against Cyber Attacks, **National Science Foundation**, Co-PI (PI: Roberto Tron), $835,405 (personal share $\approx \$417,702$), 9/2019 – 8/2023.

Building Adaptive, Dependable and Secure Systems with a Cross-Layer Weakly-Hard Paradigm, **ONR**, BU PI (Team: Northwestern + BU + UC Riverside), $190,500 (total: ∼$600,000), 10/2019 – 9/2022.

Contract-Based and Scenario-Driven Safety Analysis of Learning-Enabled Cyber-Physical Systems, **Toyota InfoTechnology Center, USA**, Sole PI, $60,000, 2018.

Safe Learning for Intelligent Transportation Systems, **Toyota InfoTechnology Center, USA**, Sole PI, $40,000, 2018.

Hariri Institute Research Incubation Award, **The Rafik B. Hariri Institute for Computing and Computational Science & Engineering**, PI (joint with Roberto Tron), $12,327 (total: $24,655), 2018.

CPS: Breakthrough: Collaborative Research: A Framework for Extensibility-Driven Design of Cyber-Physical Systems, **National Science Foundation**, Lead PI (Team: BU + Northwestern), $225,000 (total: $425,000), 9/2016 – 8/2020.

Dynamic Adaptive Embedded Software (DyAdEm), **DARPA**, BU PI (Team: SRI International + BU + Honeywell), ∼$250,000 (total: ∼$5,100,000), 7/2016 – 10/2019.

Programmers Assistant Synthesizing Code via Abstraction & Logical Inference (PASCALI), **DARPA**, BU PI (Team: SRI International + BU + MIT + University of Washington + University of Waterloo), ∼$200,000 (total: ∼$6,300,000), 7/2016 – 10/2018.

Talks and Presentations

Invited Talks/Panels

1. *Byzantine Resilience in Large Robot Swarms,*
   Invited Talk at the Department of Computer Science and Information Engineering, National Taiwan University, August 31, 2023.
2. *Achieving Verifiable Autonomy: Is Design Automation the Golden Key?*
   Panel on Autonomous Systems, Design Automation Conference, July 13, 2023.
3. *Byzantine Resilience in Large Robot Swarms,*
   Invited Talk at the Computer Science Laboratory, SRI International, July 12, 2023.
4. *Dimensions of Robustness in Deep Learning,*
   Invited Talk at the ROAD4NN Workshop, Design Automation Conference, July 9, 2023.
5. *Towards Building Safe and Trustworthy Cyber-Physical Systems,*
   Invited Talk at the CPSRC Seminar, University of California at Santa Cruz, April 20, 2023. (virtual)
6. *Byzantine Resilience in Large Robot Swarms,*
   Invited Talk at the PRECISE's Safe Autonomy Seminar, University of Pennsylvania, April 11, 2023. (virtual)
7. *Towards Building Trustworthy A.I. Systems,*
   Invited Talk at Intuit, April 5, 2023. (virtual)
8. *Specification-Driven Post-Deployment Repair of Neural Networks,*
   Invited Talk at Peking University, March 28, 2023. (virtual)

9. *Neural Trojans: Vulnerability, Detection and Defense,*
IARPA TrojAI Phase 2 Meeting, March 22, 2023. (virtual)
10. *Trojan Detection via Misattribution and Beyond,*
IARPA TrojAI Phase 2 Meeting, November 3, 2022. (virtual)
11. *Trigger-Agnostic Trojan Detection,*
IARPA TrojAI Phase 1 Meeting, June 15, 2022. (virtual)
12. *REASSURE: Sound and Complete Neural Network Repair with Minimality and Locality Guarantees,*
Invited Talk at the Dept. of Electrical and Computer Engineering, University of California at Santa Barbara, May 11, 2022. (virtual)
13. *REASSURE: Sound and Complete Neural Network Repair with Minimality and Locality Guarantees,*
Invited Talk at the Workshop on Verified Software – Verified Machine-Learning and Cyber-Physical Systems, Isaac Newton Institute for Mathematical Sciences, Cambridge, UK, July 26, 2022. (virtual)
14. *The Road to Safe Autonomy: Neural Networks Meet Formal Reasoning,*
Invited Talk at Department Colloquium, Dept. of Electrical and Computer Engineering, University of California at Riverside, November 1, 2021. (virtual)
15. *Attribution-Based Trojan Detection,*
IARPA TrojAI Kickoff Meeting, September 9, 2020. (virtual)
16. *A Framework for Extensibility-Driven Design of Cyber-Physical Systems,*
NSF CPS PI Meeting, Arlington, Virginia, November 21, 2019.
17. *(Im)proving Safety of Neural Network-Controlled Systems,*
Invited Talk at DREAM/CPAR Seminar, Dept. of Electrical Engineering and Computer Sciences, University of California at Berkeley, October 7, 2019.
18. *(Im)proving Safety of Neural Network-Controlled Systems,*
Invited Talk at United Technologies Research Center, Berkeley, October 7, 2019.
19. *(Im)proving Safety of Neural Network-Controlled Systems,*
Foundations of Safe Learning Workshop, IBM AI Research Week, Massachusetts Institute of Technology, September 20, 2019.
20. *Why Bother with Formal Methods?*
Panel on Formal Verification, MathWorks Research Summit, June 1, 2019.
21. *The Rocky Road to Safe Autonomy: A Formal Methods Perspective,*
Invited Talk at Fishbowl Seminar, Computer Engineering & Systems Group, Texas A&M University, April 25, 2019. (virtual)
22. *DyAdEm: Dynamic Adaptive Embedded Software,*
DARPA BRASS PI Meeting, Waltham, Massachusetts, August 1, 2018.
23. *Towards Assured Autonomy: From Software Architecture to Algorithm,?*
IEEE International Workshop on Design Automation for Cyber-Physical Systems, San Francisco, California, June 24, 2018.
24. *Explainable AI and Formal Methods,*
Panel on Explainable AI, MathWorks Research Summit, June 3, 2018.
25. *Simprog 2.0: Cross-Project Similarity Detection using Ontic Information,*
DARPA MUSE PI Meeting, Austin, Texas, January 23, 2018.
26. *Towards Assured Autonomy: From System Design to Algorithm,*
Invited Talk, Dept. of Computer Science, Yale University, January 19, 2018.
27. *A Framework for Extensibility-Driven Design of Cyber-Physical Systems,*
NSF CPS PI Meeting, Arlington, Virginia, November 13, 2017.

28. *Adapting Controllers Learned from Data-Driven Approaches,*
DARPA BRASS Platform Demonstration Workshop, Massachusetts Institute of Technology, February 9, 2017.
29. *Towards Dependable Robot Software,*
Dept. of Electrical Engineering, University of California at Los Angeles, Apr 4, 2016.
30. *Human-Centric Formal Methods: From Circuits to Cyber-Physical Systems,*
Given at the following venues:
    - Dept. of Electrical and Computer Engineering, Northeastern University, Apr 11, 2016.
    - Dept. of Electrical, Computer, and Energy Engineering, University of Colorado, Boulder, Apr 7, 2016.
    - Dept. of Electrical and Computer Engineering, University of British Columbia, Mar 14, 2016.
    - Dept. of Electrical and Computer Engineering, New York University, Mar 8, 2016.
    - Dept. of Electrical and Computer Engineering, Utah University, Mar 3, 2016.
    - Dept. of Electrical and Computer Engineering, Boston University, Feb 29, 2016.
    - School of Electrical and Computer Engineering, Cornell University, Feb 22, 2016.
    - Dept. of Electrical and Computer Engineering, University of Massachusetts, Amherst, Dec 4, 2015.
    - Dept. of Electrical Engineering, University of California at Los Angeles, Mar 2, 2015.
31. *Specification Mining: New Formalisms, Algorithms and Applications,*
Research in Software Engineering (RiSE), Microsoft Research, Mar 27, 2014.
32. *Dealing with the Missing Pieces: Specification Mining and Model Checking with Uncertainties,*
Computer Science Laboratory, SRI International, May 3, 2013.
33. *Analysis and Synthesis of Formal Specifications for Dependable Computing,*
Systems and Technology Group, IBM Poughkeepsie, Dec 12, 2012.
34. *Verification-Guided Soft Error Resilience,*
ASIC Engineering, NVIDIA, Feb 2009.
35. *Verification-Guided Error Resilience,*
Invited Talk at Dagstuhl Seminar on Verifying Reliability, Schloss Dagstuhl, Germany, Aug 20, 2012.

Selected Conference Presentations

36. *Safety-Aware Apprenticeship Learning,*
The 30th International Conference on Computer Aided Verification, Jul 15, 2018.
37. *Design and Verification of Multi-Rate Distributed Systems,*
The 13th ACM/IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE), Sep 21, 2015.
38. *WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates,*
IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Jun 2, 2013.
39. *Sparse Coding for Specification Mining and Error Localization,*
The 12th International Conference on Runtime Verification (RV), Sep 26, 2012.
40. *Reverse Engineering Circuits Using Behavioral Pattern Mining,*
IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Jun 3, 2012.
41. *Mining Assumptions for Synthesis,*
The 9th ACM/IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE), Jul 11, 2011.
42. *Scalable Specification Mining for Verification and Diagnosis,*
The 47th ACM/EDAC/IEEE Design Automation Conference (DAC), Jun 2010.
43. *Localizing Transient Faults Using Dynamic Bayesian Networks,*
IEEE International High Level Design Validation and Test Workshop (HLDVT), Nov 2009.

44. *Optimizations of an Application-Level Protocol for Enhanced Dependability in FlexRay,* Conference on Design, Automation and Test in Europe (DATE), Apr 2009

45. *A Theory of Mutations with Applications to Vacuity, Coverage, and Fault Tolerance,* International Conference on Formal Methods in Computer Aided Design (FMCAD), Nov 20, 2008.

Teaching Experience

Teaching at Boston University

- EC545/SE545: Cyber-Physical Systems
  - Fall 2023, Fall 2022, Fall 2021, Fall 2019
  - Graduate course on cyber-physical systems. Topics covered include specification, modeling, design, and analysis of cyber-physical systems, and applications in robotics, medical devices, and smart home and factories.
  - Created this graduate course at Boston University, taught for the first time in Fall 2019.
- EC330: Applied Algorithms for Engineers
  - Spring 2023, Spring 2022, Spring 2021, Spring 2020, Fall 2018
  - Undergraduate course on algorithms. Topics covered include the general concept of algorithms, efficiency and run-time of algorithms, graph algorithms, priority queues, search trees, various approaches to design of algorithms and data structures, together with their applications to numerical and non-numerical problems.
- EC754: Computer-Aided Verification and Synthesis
  - Fall 2020, Fall 2017
  - Advanced graduate course on computer-aided verification and synthesis. Topics covered include formal specifications, modeling formalisms, verification techniques, inductive synthesis, and emerging applications such as autonomous robots and vehicles.
  - Created this advanced graduate course at Boston University, taught for the first time in Fall 2017.
- EC535: Introduction to Embedded Systems
  - Spring 2017
  - Graduate course on embedded systems. Topics covered include system specification languages, embedded computer architecture, real-time operating systems, hardware-software co-design, modeling formalisms, verification techniques, and embedded system applications.
- EC551: Advanced Digital Design with Verilog and FPGAs
  - Fall 2016
  - Graduate course on digital design and computer-aided design algorithms for FPGAs. Topics covered include hardware description language (Verilog), specification, design, simulation, verification and synthesis of digital designs on FPGAs.

Advising and Mentoring Experience

Graduated Ph.D. students at Boston University

- Jiameng Fan (ECE), Fall 2017 – Summer 2022
  - Dissertation: *Towards Provable Safe and Robust Learning-Enabled Systems*
  - Second Place, Graduate Student Category, ACM SIGBED Student Research Competition 2021
  - First job after graduation: Software Engineer at Google
- Kacper Wardega (ECE), Fall 2017 – Summer 2023
  - Dissertation: *Securing multi-robot systems with inter-robot observations and accusations*

Ph.D. Advisees at Boston University

- Feisi Fu (SE), Fall 2019 – December 2023 (expected)
- Weichao Zhou (ECE), Fall 2018 – December 2023 (expected)

- Panagiota Kiourti (ECE), Fall 2018 – December 2023 (expected)
- H M Sabbir Ahmad (SE), Summer 2022 – Spring 2025 (expected)

M.Eng./M.S. Students at Boston University

- Harshang Umesh Chhaya (ECE), Spring 2022
- Yuhao Zhou (ECE), Summer 2020 – Fall 2020
- Shidong Sun (ECE), Summer 2019
- Xiaoyue Wang (ECE), Fall 2016 – Spring 2018
- Weichao Zhou (ECE), Fall 2016 – Spring 2018
- Hongchen Guo (ECE), Fall 2016 – Spring 2017
- Yaqin Huang (ECE), Fall 2016 – Spring 2017
- Qifan He (ECE), Summer 2017
- Akash Mehta (ECE), Spring 2017 – Spring 2018
- Muhammad Zuhayr Raghib (ECE), Spring 2017 – Spring 2018

Undergraduate Students

- Quentin Clark (ECE), Merna Alghannam (CS, UROP), Jiahui Zhu (ECE), Michael Aliberti (ECE), Zhiyuan Liu (ECE), Quinn Meurer (ECE), Madiul Chowdhury (ECE), Jennifer Norell (ECE)

Visiting Undergraduate Students

- Ruihan Gao (Nanyang Technological University), Summer 2019
- Panyang Qi (Peking University), Summer 2018
- Yishuang Lin (University of Science and Technology of China), Summer 2018

High School Students

- Tarang Gaddam (BU RISE Intern), Summer 2023
- Andy Cheng (BU RISE Intern), Summer 2022
- Nashita Rahman (BU RISE Intern), Summer 2019
- Edward Yang (BU RISE Intern), Summer 2018
- Eddie Hew (BU RISE Intern), Summer 2017

Ph.D. Prospectus/Dissertation Committees

- Ziqi Yang (ME), Defense in Summer 2023
- Yangruirui Zhou, Prospectus in Summer 2023
- Max Cohen (ME), Defense in Spring 2023
- Kasra Ghasemi (SE), Defense in Fall 2022
- Suhail Alsalehi (SE), Defense in Fall 2022
- Shiza Ali (ECE), Prospectus in Fall 2022
- Mohammad Hammas Saeed (ECE), Prospectus in Fall 2022
- Rushi Patel (ECE), Defense in Summer 2022
- Guang Yang (ME), Defense in Summer 2020
- Emre Ates (ECE), Defense in Summer 2020
- Yenai Ma (ECE), Defense in Spring 2020
- Francisco Penedo (SE), Defense in Spring 2020
- Giuseppe Bombara (ECE), Defense in Fall 2019
- Iman Haghighi (ME), Defense in Spring 2019
- Xiao Li (ME), Defense in Fall 2019

- Prashant Vaidyanathan (ECE), Defense in Fall 2019
- Sadra Sadraddini (ME), Defense in Fall 2017

M.S. Thesis Committees

- Pierre-François Wolfe (ECE), Defense in Spring 2021
- Anthony Ducimo (ECE), Defense in Fall 2020
- Xinwei Zhang (ME), Defense in Spring 2020
- Weichao Zhou (ECE), Defense in Spring 2018, as Advisor
- Yannan Bai (ECE), Defense in Spring 2018
- Kiran Vishal Thanjavur Bhaaskar (ECE), Defense in Spring 2017

Professional Services

Editorial Boards

- Associate Editor, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022 – present.
- Associate Editor, Electronic Newsletter, ACM Special Interest Group on Design Automation, 2019.
- Guest Editor, Special Issue on (Industrial) Internet of Things for Smart & Sensing Systems: Issues, Trends and Applications, IEEE Internet of Things Journal, 2018.
- Guest Editor, Special Issue on Cyber-Physical Aspects of EVs and HEVs, IET Cyber-Physical Systems: Theory & Applications, 2017.

Conference and Workshop Organization

- Chair, Embedded, Cyberphysical (CSP), IoT Systems and Software Track, The 29th Asia and South Pacific Design Automation Conference (ASP-DAC), 2024.
- Organizer, Early Career Workshop, The 60th ACM/EDAC/IEEE Design Automation Conference (DAC), 2023.
- Organizer, Tutorials on Virtual and Scenario-Based Testing of Autonomous Systems, The 60th ACM/EDAC/IEEE Design Automation Conference (DAC), 2023.
- Organizer, Tutorials on Architectures and Machine Learning Models for High-Assurance Autonomous Systems, The 60th ACM/EDAC/IEEE Design Automation Conference (DAC), 2023.
- Chair, Autonomous Systems Track, The 60th ACM/EDAC/IEEE Design Automation Conference (DAC), 2023.
- Chair, Embedded, Cyberphysical and IoT Systems Track, The 28th Asia and South Pacific Design Automation Conference (ASP-DAC), 2023.
- Chair, The 31st ACM SIGDA University Demonstration, 2021.
- Chair, Autonomous Systems Track, The 58th ACM/EDAC/IEEE Design Automation Conference (DAC), 2021.
- Organizer, Panel on Design of Autonomous Systems, The 57th ACM/EDAC/IEEE Design Automation Conference (DAC), 2020.
- Organizer, Special Session on Safe Autonomy, The 38th ACM/IEEE International Conference on Computer-Aided Design (ICCAD), 2019.
- Publicity Chair, The 30th ACM SIGDA University Demonstration at DAC, 2018.
- Session Chair, Special Session on CAD for Next-Generation Vehicles, The 33rd ACM/IEEE International Conference on Computer Aided Design (ICCAD), 2014.

Technical Program Committee

- Member, The 15th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2024
- Member, The 29th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2023

- Member, The 41st International Conference on Computer-Aided Design (ICCAD), 2022.
- Member, The 52nd IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2022.
- Member, Conference on Design, Automation and Test in Europe (DATE), 2022.
- Member, The 27th Asia and South Pacific Design Automation Conference (ASP-DAC), 2022.
- Member, The 40th ACM/IEEE International Conference on Computer Aided Design (ICCAD), 2021.
- Member, Conference on Design, Automation and Test in Europe (DATE), 2021.
- Member, The 51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021.
- Member, The 23rd ACM International Conference on Hybrid Systems: Computation and Control (HSCC), 2020.
- Member, The 57th ACM/EDAC/IEEE Design Automation Conference (DAC), 2020.
- Member, International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2020.
- Member, Conference on Design, Automation and Test in Europe (DATE), 2020.
- Member, The 56th ACM/EDAC/IEEE Design Automation Conference (DAC), 2019.
- Member, The 55th ACM/EDAC/IEEE Design Automation Conference (DAC), 2018.
- Member, The 37th ACM/IEEE International Conference On Computer Aided Design (ICCAD), 2018.
- Member, ACM SIGBED International Conference on Embedded Software (EMSOFT), 2018.
- Member, The 9th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2018.
- Member, The 9th NASA Formal Methods Symposium (NFM), 2017.
- Member, Conference on Design, Automation and Test in Europe (DATE), 2017.
- Member, Automated Formal Methods Workshop (AFM), 2017.
- Member, The 4th Workshop on Design Automation for Understanding Hardware Designs (DUHDe), 2017.
- Member, The 13th IEEE International Conference on Embedded Software and Systems (ICESS), 2016.
- Member, The 3rd Workshop on Design Automation for Understanding Hardware Designs (DUHDe), 2016.
- Member, The 12th IEEE International Conference on Embedded Software and Systems (ICESS), 2015.
- Member, International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS), 2015.
- Member, The 1st Workshop on Design Automation for Understanding Hardware Designs (DUHDe), 2014.

Other Professional Services

- NSF Panel.

University and Department Services

- Faculty Mentor, Research in Science & Engineering (RISE) Program, Boston University, 2017 – Present
- Publicity Committee, ECE Department, Boston University, 2017 – 2020
- Doctoral Committee, ECE Department, Boston University, 2022 – 2023, 2016 – 2020
- Master Committee, ECE Department, Boston University, 2020 – 2022, 2016 – 2017