MENGYU LIU

+1 315-800-8172, mliu9@nd.edu, https://mengyuliu0520.github.io/

RESEARCH SUMMARY

My research interests are Cyber-Physical System(CPS), machine learning and security problems. My aim is to maintain the safety of CPS in real-time with guarantee. I believe the integration of model-based methods, formal methods and learning-based techniques will help achieve this goal.

PROFESSIONAL EXPERIENCE

University of Notre Dame, South bend, IN, USA 2023 - present
Teaching Assistant, College of Engineering & Computer Science

Syracuse University, Syracuse, NY, USA 2021 - 2023
Teaching Assistant, College of Engineering & Computer Science

Syracuse University, Syracuse, NY, USA 2020 - 2021
Research Assistant, College of Engineering & Computer Science

Syracuse University, Syracuse, NY, USA 2019 - 2020
Faculty Assistant, School of Information Studies

Syracuse University, Syracuse, NY, USA 2019
Summer Research Intern, School of Information Studies

EDUCATION

Ph.D., Computer Engineering(Transferred from SU) 2023 - present
University of Notre Dame, South bend, IN, USA

Ph.D., Computer and Information Science and Engineering 2020 - 2023
Syracuse University, Syracuse, NY, USA

M.S., Computer and Information Science and Engineering 2018 - 2020
Syracuse University, Syracuse, NY, USA

B.S., Computer Science 2014 - 2018
University of Toronto, Toronto, ON, Canada

AWARDS

Artificial Intelligence Maritime Maneuver Indiana Collegiate Challenge 1st Place	2024
Oral Presentation in COSE Research Horizons Symposium at Notre Dame (16/100)	2023
Summer Pre-disseration Fellowship $4000 (4/110)	2023
SIGBED Student Travel Grant for CPS-IoT week	2023
DAC Young Fellow	2020
RTSS Student Travel Grant	2022
Syracuse University Tuition Waiver	2018 - 2020

PUBLICATIONS

Book Chapters:

[b.1] Lin Zhang, **Mengyu Liu**, Fanxin Kong. ”AI-enabled Real-time Sensor Attack Detection for Cyber-physical Systems”, a chapter in AI Embedded Assurance for Cyber Systems, Springer, 2023.

Journal Articles:

[j.3] **Mengyu Liu**, Lin Zhang, Weizhe Xu, Shixiong Jiang, Fanxin Kong, 2023. CPSim: Simulation Toolbox for Security Problems in Cyber-Physical Systems. Accepted by ACM Transactions on Design Automation of Electronic Systems.

[j.2] M Hani Sulieman, **Mengyu Liu**, M Cenk Gursoy, Fanxin Kong, 2023. Path Planning for UAVs Under GPS Permanent Faults. Accepted by ACM Transactions on Cyber-Physical Systems.

[j.1] Pengyuan Lu, Lin Zhang, **Mengyu Liu**, Kaustubh Sridhar, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2022.

Recovery from Adversarial Attacks in Cyber-physical Systems: Shallow, Deep and Exploratory Research. Accepted by ACM Computing Surveys.

Conference Papers:

[c.14] Weizhe xu, **Mengyu Liu**, Oleg Sokolsky, Insup Lee, Fanxin Kong. LLM-enabled Cyber-Physical Systems: Survey, Research Opportunities, and Challenges. International Workshop on Foundation Models for Cyber-Physical Systems & Internet of Things (FMSys) 2024.

[c.13] **Mengyu Liu**, Pengyuan Lu, Xin Chen, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2024. Deadline-Safe Reach-Avoid Control Synthesis for Cyber-Physical Systems with Reinforcement Learning. Under review at IEEE Real-Time Systems Symposium (RTSS'24)

[c.12] Md Kausar Hamid Miji, **Mengyu Liu**, Francis Akowuah, Fanxin Kong. Work in Progress: Emerging From Shadows: Optimal Hidden Actuator Attack to Cyber-Physical Systems. Accepted IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2024.

[c.11] Shixiong Jiang, **Mengyu Liu**, Fanxin Kong. Demo: Vulnerability Analysis for STL-Guided Safe Reinforcement Learning in Cyber-Physical Systems. Accepted IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2024.

[c.10] Weizhe Xu, **Mengyu Liu**, Steven Drager, Matthew Anderson, Fanxin Kong. Poster Abstract: Assuring LLM-Enabled Cyber-Physical Systems. Accepted by International Conference on Cyber Physical Systems (ICCPS'24).

[c.9]Jean Park*, Sydney Pugh*, Kaustubh Sridhar, **Mengyu Liu**, Ramneet Kaur, Souradeep Dutta, Elena Bernadis, Oleg Sokolsky, Insup Lee. Automating Weak Label Generation for Data Programming with Clinicians in the Loop. Accepted by IEEE/ACM international conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) 2024.

[c.8] Lin Zhang, **Mengyu Liu**, Fanxin Kong, 2024. Security Toolbox for Cyber-Physical Systems. In Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) brief presentation.

[c.7] Shixiong Jiang*, **Mengyu Liu***, Fanxin Kong, 2024. Vulnerability Analysis for Temporal Logic Guided Safe Reinforcement Learning in Cyber-Physical Systems. Accepted by International Conference on Cyber Physical Systems (ICCPS'24).

[c.6] **Mengyu Liu***, Pengyuan Lu*, Xin Chen, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2024. Model-free PAC Time-Optimal Control Synthesis with Reinforcement Learning. Accepted by ACM/IEEE International Symposium on Formal Methods and Models for System Design (MEMOCODE'24).

[c.5] **Mengyu Liu**, Pengyuan Lu, Xin Chen, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2023. Fulfilling Formal Specifications ASAP by Model-free Reinforcement Learning. Preprint in arXiv.

[c.4] **Mengyu Liu**, Lin Zhang, Vir Phoha, Fanxin Kong, 2023. Learn-to-Respond: Sequence-Predictive Recovery from Sensor Attacks in Cyber-Physical Systems. Accepted by IEEE Real-Time Systems Symposium (RTSS'23).

[c.3] Lin Zhang, Kaustubh Sridhar, **Mengyu Liu**, Pengyuan Lu, Xin Chen, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2023. Real-Time Data-Predictive Attack-Recovery for Complex Cyber-Physical Systems. In Proceedings of IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'23).

[c.2] **Mengyu Liu**, Lin Zhang, Pengyuan Lu, Kaustubh Sridhar, Fanxin Kong, Oleg Sokolsky, Insup Lee, 2022. Fail-Safe: Securing Cyber-Physical Systems against Hidden Sensor Attacks. In Proceedings of the IEEE Real-Time Systems Symposium (RTSS'22). 240-252.

[c.1] Lin Zhang, Zifan Wang, **Mengyu Liu**, Fanxin Kong, 2022. Adaptive Window-Based Sensor Attack Detection for Cyber-Physical Systems.In Proceedings of the ACM/IEEE Design Automation Conference (DAC'22). 919-924.

TEACHING EXPERIENCE

University of Notre Dame	
CSE40728 - System Design and Implementation of Small Autonomous Vehicles	Spring 2024
CSE60641 - Operating Systems	Fall 2023
Syracuse University CIS655 - Computer Architecture	Spring 2023
CIS655 - Computer Architecture	Fall 2022
CIS341 - Computer Organization & Programming Systems	Spring 2022
CIS655 - Computer Architecture	Fall 2021
CIS675 - Design&Analysis of Algorithms	Fall 2019

IST718 - Big Data Analytics	Summer 2019

KEY COURSEWORKS

Machine Learning, Scientific Computing, Data Structures and Algorithms, Computer Vision, Optimization, Operating Systems, Formal Methods, Game Theory, Biometrics

TECHNICAL SKILLS

Langugaes: Python, Matlab, C++, C, Haskell, HTML, Assembly, R

Robotics: MuJoCo, ROS2

Machine Learning: PyTorch, OpenAI Gym, Tensorflow, Keras, Sklearn

Data Science: Spark, MySQL, Pandas

MENTORING EXPERIENCE

Graduate Students:

Tian Jiang, Syracuse University.	Spring 2022
Zhuowei Zhang, Syracuse University.	Spring 2022
Youdan Zhang, Syracuse University. (now at Fortinet)	Fall 2021 - Spring 2022
Tianshu Ren, Syracuse University. (now at Silicon Labs)	Fall 2021
Ruiji Wei, Syracuse University. (now at Morgan Stanley)	Fall 2020 - Spring 2021
Yueyuan He, Syracuse University. (now at Cisco)	Fall 2020 - Spring 2021

Undergraduate Students:

Yujie Xu, Syracuse University.	Fall 2022
Runzhou Chen, Syracuse University. (now M.S student at John Hopkins University)	Summer 2022
Xinqian Zhou, Syracuse University. (now M.S student at Brown University)	Fall 2021 - Spring 2022
Xiaofeng Pan, Syracuse University. (now M.S student at University of South California)	Fall 2021 - Spring 2022
Jiaqi Li, Syracuse University. (now M.S student at University of South California)	Fall 2021-Spring 2022
Arvin Lee, Syracuse University.	Fall 2020 - Spring 2021
Chengyuan Zhang, Syracuse University. (now M.S student at CMU)	Spring 2019 - Spring 2021
Hao Li, Syracuse University.	Spring 2019 - Spring 2021
Shutong Wu, Syracuse University. (now M.S student at UPenn)	Spring 2019 - Spring 2020

SERVICE

Education Service:

Instructor for OrangeWorks Summer Program for High School Students

Coach for Artificial Intelligence Maritime Maneuver Indiana Collegiate Challenge

Reviewers for Journals:

IEEE Internet Computing

IEEE Internet of Things Journal

Springer Discover Internet of Things

IEEE Transactions on Smart Grid

Subreviewer for Journals:

Journal of Systems Architecture

Internet of Things Journal

Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

Transactions on Cyber-Physical Systems (TCPS)

Subreviewer for Conferences:

Real-Time Systems Symposium (RTSS'24)

Design Automation Conference (DAC'24)

International Conference on Future Energy Systems (e-energy'23)

Real-Time Systems Symposium (RTSS'22)

Design Automation Conference (DAC'22)

Real-Time and Embedded Technology and Applications Symposium (RTAS'22)
Design, Automation and Test in Europe Conference (DATE'21)
International Conference on Electronic Spectroscopy and Structure(ICESS'21)
International Symposium On Real-Time Distributed Computing (ISORC'21)
Real-Time and Embedded Technology and Applications Symposium (RTAS'21)
International Conference on Cyber-Physical Systems (ICCPS'21)
Real-Time Systems Symposium (RTSS'20)
International Conference on Embedded Software (EMSOFT'20) WIP
International Symposium on Quality of Service (IWQoS'20)
International Conference on Future Energy Systems (e-energy'20)
European Conference on Wireless Sensor Networks (EWSN'20) poster

CERTIFICATE

Federal Aviation Administration(FAA) 2022
Part 107 Small Uas Initial - Part 61 Pilots