Lin Zhang

zl@ieee.org | https://linzhang.org/ | M0-Q62sAAAAJ | lin-zhang-cps | lion-zhang

Education

Syracuse University — Syracuse, NY

M.S. in Computer Science; GPA: 4.00/4.00 — *May 2022*

Ph.D. in Computer and Information Science and Engineering; GPA: 4.00/4.00 — *May 2023*

- **Dissertation:** Real-time Adaptive Detection and Recovery Against Sensor Attacks in Cyber-physical Systems
- **Advisor:** Fanxin Kong

Dalian University of Technology — Dalian, China

B.E. in Computer Science and Technology; GPA: 3.76/4.0, Rank: 3/96 — *July 2015*

Research

Research Interests

Cyber-physical Systems	Security and Safety	Sensor Attacks
Autonomous Systems	Attack Detection	Attack Recovery

Journal Articles

[1] P. Lu, **L. Zhang**, M. Liu, K. Sridhar, O. Sokolsky, F. Kong, and I. Lee. "Recovery from Adversarial Attacks in Cyber-physical Systems: Shallow, Deep and Exploratory Works". In: *ACM Comput. Surv.* CS (Mar. 2024). Just Accepted. ISSN: 0360-0300. DOI: 10.1145/3653974. https://doi.org/10.1145/3653974.

[2] **L. Zhang***, Z. Wang*, and F. Kong. "Optimal Checkpointing Strategy for Real-Time Systems with Both Logical and Timing Correctness". In: *ACM Trans. Embed. Comput. Syst.* TECS '23 22.4 (July 2023). ISSN: 1539-9087. DOI: 10.1145/3603172. https://doi.org/10.1145/3603172.

[3] Y. Chen, T. Zhang, F. Kong, **L. Zhang**, and Q. Deng. "Attack-Resilient Fusion of Sensor Data with Uncertain Delays". In: *ACM Trans. Embed. Comput. Syst.* TECS '22 (Mar. 2022). ISSN: 1539-9087. DOI: 10.1145/3532181. https://doi.org/10.1145/3532181.

[4] **L. Zhang**, P. Lu, F. Kong, X. Chen, O. Sokolsky, and I. Lee. "Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear-Quadratic Regulator". In: *ACM Trans. Embed. Comput. Syst.* EMSOFT '21 20.5s (Sept. 2021). ISSN: 1539-9087. DOI: 10.1145/3477010. https://doi.org/10.1145/3477010.

Refereed Conference Proceedings

[5] **L. Zhang***, L. Burbano*, X. Chen, A. A. Cardenas, S. Drager, M. Anderson, and F. Kong. "Fast Attack Recovery for Stochastic Cyber-Physical Systems". In: *2024 IEEE 30th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. RTAS '24. 2024.

[6] M. Liu, **L. Zhang**, V. V. Phoha, and F. Kong. "Learn-to-Respond: Sequence-Predictive Recovery from Sensor Attacks in Cyber-Physical Systems". In: *2023 IEEE Real-Time Systems Symposium (RTSS)*. RTSS '23. 2023, pp. 78–91. DOI: 10.1109/RTSS59052.2023.00017.

[7] Z. Wang, **L. Zhang**, Q. Qiu, and F. Kong. "Catch You if Pay Attention: Temporal Sensor Attack Diagnosis Using Attention Mechanisms for Cyber-Physical Systems". In: *2023 IEEE Real-Time Systems Symposium (RTSS)*. RTSS '23. 2023, pp. 64–77. DOI: 10.1109/RTSS59052.2023.00016.

[8] **L. Zhang**, K. Sridhar, M. Liu, P. Lu, X. Chen, F. Kong, O. Sokolsky, and I. Lee. "Real-Time Data-Predictive Attack-Recovery for Complex Cyber-Physical Systems". In: *2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. RTAS '23. 2023, pp. 209–222. DOI: 10.1109/RTAS58335.2023.00024.

[9] M. Liu, **L. Zhang**, P. Lu, K. Sridhar, F. Kong, O. Sokolsky, and I. Lee. "Fail-Safe: Securing Cyber-Physical Systems against Hidden Sensor Attacks". In: *2022 IEEE Real-Time Systems Symposium (RTSS)*. RTSS '22. 2022, pp. 240–252. DOI: 10.1109/RTSS55097.2022.00029.

[10] **L. Zhang**, Z. Wang, M. Liu, and F. Kong. "Adaptive Window-Based Sensor Attack Detection for Cyber-Physical Systems". In: *Proceedings of the 59th ACM/IEEE Design Automation Conference*. DAC '22. San Francisco, California: Association for Computing Machinery, 2022, pp. 919–924. ISBN: 9781450391429. DOI: 10.1145/3489517.3530555. https://doi.org/10.1145/3489517.3530555.

[11] T. He, **L. Zhang**, F. Kong, and A. Salekin. "Exploring Inherent Sensor Redundancy for Automotive Anomaly Detection". In: *2020 57th ACM/IEEE Design Automation Conference (DAC)*. DAC '20. 2020, pp. 1–6. DOI: 10.1109/DAC18072.2020.9218557.

[12] **L. Zhang**, X. Chen, F. Kong, and A. A. Cardenas. "Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear Approximations". In: *2020 IEEE Real-Time Systems Symposium (RTSS)*. RTSS '20. 2020, pp. 205–217. DOI: 10.1109/RTSS49844.2020.00028.

Book Chapters

[13] **L. Zhang**, M. Liu, and F. Kong. "AI-enabled Real-Time Sensor Attack Detection for Cyber-Physical Systems". In: *AI Embedded Assurance for Cyber Systems*. Ed. by C. Wang, S. Iyengar, and K. Sun. Book. Cham: Springer International Publishing, 2023, pp. 91–120. ISBN: 978-3-031-42637-7. DOI: 10.1007/978-3-031-42637-7_6. https://doi.org/10.1007/978-3-031-42637-7_6.

Workshop & Work-in-Process

[14] **L. Zhang**, M. Liu, and F. Kong. "Demo: Simulation and Security Toolbox for Cyber-Physical Systems". In: *2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. RTAS '23. Los Alamitos, CA, USA: IEEE Computer Society, May 2023, pp. 357–358. DOI: 10.1109/RTAS58335.2023.00040. https://doi.ieeecomputersociety.org/10.1109/RTAS58335.2023.00040.

[15] **L. Zhang**, Z. Wang, and F. Kong. "Work-in-Progress: Optimal Checkpointing Strategy for Real-time Systems with Both Logical and Timing Correctness". In: *2022 IEEE Real-Time Systems Symposium (RTSS)*. RTAS '22. 2022, pp. 515–518. DOI: 10.1109/RTSS55097.2022.00055.

Current Project

Real-time Sensor Attack Detection and Recovery for Cyber-physical Systems (CPS)

- **Attack detection:** explores sensor redundancy and identifies sensor attacks against CPS in real-time, studies adaptive sensor attack detection under different system states, and explores alerts on hidden attacks.
- **Attack recovery:** formulates the attack recovery problem as optimization problems to find a recovery control sequence that can steer system states back to the target set before a safe deadline.

Awards & Achievements

- "The Pramod K. and Anju Varshney Endowed Graduate Scholarship for the 2022-2023 academic year", Syracuse University, March 2023.
- "Best Scientific Research Award of ACM SIGBED Student Research Competition (SRC) 2022", October 2022.
- "1st place in Oral Presentation Competition at 2022 ECS Research Day", Syracuse University, College of Engineering & Computer Science, March 2022
- "Syracuse University Fellowship", Syracuse University, 2019–2020, 2021–2022
- "1st place Overall College Poster Prize in 2020 ECS Research Day", Syracuse University, College of Engineering & Computer Science, November 2020
- "Merit Student & Excellent Student Cadre of UCAS," University of Chinese Academy of Sciences, June 2016.
- "Best Creative Project of the 7th National Conference of Undergraduate on Innovation and Entrepreneurship," China, October 2014.
- "National Scholarship & Outstanding League Cadres of DUT", Dalian University of Technology, 2013-2014.
- "1st Prize of "TI Cup" Liaoning College Students Electronic Design Competition", China, September 2013.

Work Experience

University of Pennsylvania Philadelphia, PA

Postdoctoral Researcher *Sep 2023 – Present, Full-time*

- Currently working with Prof. Insup Lee in the PRECISE Center.
- Developing fast sensor attack recovery for stochastic CPS, exploring attack detection and recovery codesign.

Syracuse University Syracuse, NY

Teaching Assistant *Aug 2022 – May 2023*

- Graduate Course: Principles of Operating Systems (CIS 657)
- Undergraduate Course: Design of Operating Systems (CSE/CIS 486)

Syracuse University Syracuse, NY

Research Assistant *Jun 2020 – August 2021*

- Proposed optimization-based real-time attack recovery method for CPS.
- Designed and implemented the experimental robotic vehicle testbed.
- Developed simulation and security toolbox for CPS — CPSim

Last updated on March 28, 2024.