

Tao Li

City University of Hong Kong
Yeung Kin Man Academic Building
83 Tat Chee Avenue, Hong Kong

Email: li.tao@cityu.edu.hk
Phone: +852 3442 7310
Web: <https://taoli-nyu.github.io>

EDUCATION

New York University

Brooklyn, NY

Ph.D. in Electrical and Computer Engineering

Sept. 2018 – May 2025

- Dissertation: Computational Foundations of Multi-Agent Learning in Cyber-Physical-Human Networks under Amorphous Information Attributes (Available at Proquest)
- Advisor: Prof. Quanyan Zhu; Committee: Prof. Sundeep Rangan, Prof. Kaan Özbay
- Awards: Dante Youla Award for Research Excellence 2024

Xiamen University

Fujian, China

B.S. in Mathematics, summa cum laude

Sept. 2014 – Jun. 2018

- Awards: National Scholarship by Ministry of Education of China

PROFESSIONAL EXPERIENCE

City University of Hong Kong

Hong Kong

Assistant Professor

Sept. 2025 – Present

- Department of Systems Engineering, College of Engineering

IBM Research

Yorktown Heights, NY

Visiting Researcher

Jun. 2025 – Aug. 2025

- Mathematical Sciences

University of Illinois Urbana Champaign

Champaign, IL

Visiting Scholar

Jul. 2024 – Aug. 2024

- Coordinated Science Laboratory, Host: Prof. Tamer Başar

New York University

Brooklyn, NY

Research Assistant

Sept. 2018 – May 2025

- NYU Center for Cybersecurity, NYU Wireless, NYU C2SMARTER Center

University of Alberta

Alberta, Canada

Research Assistant

May 2017 – Oct. 2017

- Department of Mathematical and Statistical Sciences, Host: Prof. Bin Han

AWARDS

Best Paper Award, ALA@AAMAS2025

2025

- Awarded by the 17th Workshop on Adaptive and Learning Agents in conjunction with 24th International Conference on Autonomous Agents and Multiagent Systems.

NSF Division of Mathematical Sciences (DMS) Travel Grant

2025

- Awarded by NSF DMS for presenting at the workshop on *Uncertainty Quantification Strategies for Multi-Physics Systems and Digital Twins* at the Institute for Mathematical and Statistical Innovation (IMSI). Selected as the only graduate student to present among early-career researchers.

NSF NeTS Early Career Investigators (ECI) Workshop Travel Grant

2025

- Awarded by NSF NeTS Program for attending the NeTS-ECI workshop at the NSF headquarters.

Rising Star in AI and Machine Learning in Security

2024

- Awarded by the IEEE ComSoc special interest group for AI and machine learning in security.
- Society for Industrial and Applied Mathematics Travel Award** 2024
- Awarded by SIAM for attending the Conference on Mathematics of Data Science.
- Dante Youla Award For Research Excellence** 2024
- Awarded by Dept. ECE in recognition of graduate research excellence.
- MidWest Control and Game Theory Conference Travel Award** 2024
- Awarded by the University of Minnesota for conference presentations.
- Game Theory and AI for Security Conference Travel Award** 2022
- Awarded by Carnegie Mellon University for conference presentations.
- Best Student Paper Finalist, IEEE MLSP** 2019
- One of the ten finalists at International Workshop on Machine Learning for Signal Processing.
- Mitacs-Globalink Research Award** 2017
- Awarded by Natural Sciences and Engineering Research Council of Canada for undergrad research.
- National Scholarship** 2015
- Awarded by the Ministry of Education of China for undergrad academic excellence.

PUBLICATIONS

* indicates equal contribution; † indicates mentees.

Book Chapters

- [B2] T. Li and Q. Zhu, “Symbiotic game and foundation models for cyber deception operations in strategic cyber warfare,” in *Foundations of Cyber Deception: Modeling, Analysis, Design, Human Factors and Their Convergence*, Advances in Information Security, Springer Cham, Aug. 2025.
- [B1] T. Li, Y. Pan, and Q. Zhu, “Decision-dominant strategic defense against lateral movement for 5G zero-trust multi-domain networks,” in *Network Security Empowered by Artificial Intelligence*, Advances in Information Security, vol. 107, pp. 25-76, Springer Cham, Feb. 2024.

Journals

- [J9] T. Li, Z. Bian, H. Lei, F. Zuo, Y-T. Yang, Q. Zhu, Z. Li, Z. Chen, and K. Ozbay, “Digital twin-based driver risk-aware predictive mobility analytics for real-time situational awareness through cooperative sensing,” *IEEE Transactions on Intelligent Transportation Systems*, Early Access, 2025.
- [J8] Y-T. Yang, T. Li, and Q. Zhu, “Transparent tagging for strategic social nudges on user-generated misinformation,” *IEEE Transactions on Network Science and Engineering*, Early Access, 2025.
- [J7] K. Hammar*, T. Li*, R. Stadler, and Q. Zhu, “Automating security strategies through online learning with adaptive conjectures,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 4055-4070, 2025.
- [J6] T. Li, H. Lei, H. Guo, M. Yin, Y. Hu, Q. Zhu, and S. Rangan, “Digital twin-enhanced wireless indoor navigation: Achieving efficient environment sensing with zero-shot reinforcement learning,” *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2356-2372, 2025.
- [J5] T. Li, Z. Bian, H. Lei, F. Zuo, Y-T. Yang, Q. Zhu, Z. Li, and K. Ozbay, “Multi-level traffic-responsive tilt camera surveillance through predictive correlated online learning,” *Transportation Research Part C: Emerging Technologies*, vol. 167, 2024.
- [J4] S. Liu, T. Li, and Q. Zhu, “Game-theoretic distributed empirical risk minimization with strategic network design,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 9, pp. 542-556, 2023.
- [J3] T. Li, Y. Zhao, and Q. Zhu, “The role of information structures in game-theoretic multi-agent learning,” *Annual Reviews in Control*, vol. 53, pp. 296-314, 2022.

- [J2] T. Li, G. Peng, Q. Zhu, and T. Başar, “The confluence of networks, games, and learning a game-theoretic framework for multi-agent decision making over networks,” *IEEE Control Systems*, vol. 42, no. 4, pp. 35-67, 2022.
- [J1] B. Han*, T. Li*, X. Zhuang*, “Directional compactly supported box spline tight framelets with simple geometric structure,” *Applied Mathematics Letters*, vol. 91, pp. 213-219, 2019.

Conferences

- [C16] K. Hammar and T. Li, “Online incident response planning under model misspecification through Bayesian learning and belief quantization,” in *Proceedings of the 2025 Workshop on Artificial Intelligence and Security (AISec’25)*, Taipei, Taiwan, Oct. 2025.
- [C15] T. Li, H. Lei, M. Yin, and Y. Hu, “Reinforcement learning with physics-informed symbolic program priors for zero-shot wireless indoor navigation,” in *2025 Reinforcement Learning Conference (RLC’25), Workshop on Inductive Bias in Reinforcement Learning*, Edmonton, Canada, Aug. 2025.
Spotlight, Best Paper Award Runner Up, 3/14 accepted papers.
- [C14] T. Li, J. Guevara, X. Xie, and Q. Zhu, “Self-confirming transformer for belief-conditioned adaptation in offline multi-agent reinforcement learning,” in *24th International Conference on Autonomous Agents and Multiagent Systems (AAMAS’25), 7th Workshop on Adaptive and Learning Agents*, Detroit, MI, USA, May, 2025.
Best Paper Award Runner Up, 2/45 accepted papers.
- [C13] T. Li, K. Hammar, R. Stadler, and Q. Zhu, “Conjectural online learning with first-order beliefs in asymmetric information stochastic games,” in *63rd IEEE Conference on Decision and Control (CDC’24)*, Milan, Italy, Dec. 2024.
- [C12] Y. Pan, T. Li, and Q. Zhu, “On the variational interpretation of mirror play in monotone games,” in *63rd IEEE Conference on Decision and Control (CDC’24)*, Milan, Italy, Dec. 2024.
- [C11] M. Yin, T. Li, H. Lei, Y. Hu, S. Rangan, and Q. Zhu, “Zero-shot wireless indoor navigation through physics-informed reinforcement learning,” in *IEEE International Conference on Robotics and Automation (ICRA’24)*, Yokohama, Japan, May 2024.
- [C10] Y. Pan*, T. Li*, H. Li, T. Xu, Z. Zheng, and Q. Zhu, “A first-order meta Stackelberg method for robust federated learning,” in *40th International Conference on Machine Learning, Adversarial Machine Learning Workshop (ICML AdvML Wkshp 2023)*, Honolulu, HI, USA, Jul. 2023.
- [C9] T. Li and Q. Zhu, “On the price of transparency: A comparison between overt persuasion and covert signaling,” in *62nd IEEE Conference on Decision and Control (CDC’23)*, Singapore, Dec. 2023.
- [C8] Y. Pan, T. Li, and Q. Zhu, “Is stochastic mirror descent vulnerable to adversarial delay attacks? A traffic assignment resilience study,” in *62nd IEEE Conference on Decision and Control (CDC’23)*, Singapore, Dec. 2023.
- [C7] Y-T. Yang*, T. Li*, and Q. Zhu, “Designing policies for truth: Combating misinformation with transparency and information design,” in *21st International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt’23)*, Singapore, Aug. 2023.
- [C6] Y. Ge*, T. Li*, and Q. Zhu, “Scenario-agnostic zero-trust defense with explainable threshold policy: A meta-learning approach,” in *IEEE Conference on Computer Communications (INFOCOM Wkshp 2023)*, Hoboken, NJ, USA, May 2023.
- [C5] Y. Pan, T. Li, and Q. Zhu, “On the resilience of traffic networks under non-equilibrium learning,” in *American Control Conference (ACC’23)*, San Diego, CA, USA, May 2023.
- [C4] T. Li, H. Lei and Q. Zhu, “Self-adaptive driving in nonstationary environments through conjectural online lookahead adaptation,” in *IEEE International Conference on Robotics and Automation (ICRA’23)*, London, United Kingdom, May 2023.
- [C3] G. Peng, T. Li, S. Liu, J. Chen, and Q. Zhu, “Locally-aware constrained games on networks,” in *American Control Conference (ACC’21)*, virtual, May 2021.

- [C2] T. Li, G. Peng and Q. Zhu, “Blackwell online learning for Markov decision processes,” in *55th Annual Conference on Information Sciences and Systems (CISS’21)*, virtual, Mar. 2021.
- [C1] T. Li and Q. Zhu, “On convergence rate of adaptive multiscale value function approximation for reinforcement learning,” in *29th IEEE International Workshop on Machine Learning for Signal Processing (MLSP Wkshp 2019)*, Pittsburgh, PA, USA, Oct. 2019.

Preprints

- [P3] T. Li, H. Li, Y. Pan, T. Xu, Z. Zheng, and Q. Zhu, “Meta Stackelberg game: Robust federated learning against adaptive and mixed poisoning attacks,” submitted to *IEEE Transactions on Information Forensics and Security*, 2024.
- [P2] T. Li and Q. Zhu, “Commitment with signaling under double-sided information asymmetry,” arXiv preprint, 2022, arXiv:2212.11446.
- [P1] B. James*, B. Windsor*, W. Song*, and T. Li*, “Causality and batch reinforcement learning: Complementary approaches to planning in unknown domains,” arXiv preprint, 2020, arXiv:2006.02579.

INVITED TALKS

- [T13] “Asymptotics of Bayesian Reinforcement Learning under Model Misspecification,” at *IBM Thomas J. Watson Research Center*, Yorktown Heights, NY, Jun. 20, 2025.
- [T12] “Digital-Twin-Enabled Predictive Traffic Sensing via Multi-Agent Risk-Constrained Online Learning,” at *Annual East Coast Optimization Meeting, Center for Mathematics and Artificial Intelligence, George Mason University*, Arlington, VA, Apr. 17, 2025.
- [T11] “Risk-Aware Long-Short-Term Adaptive Twinning in Urban Traffic Digital Twin,” at *Institute for Mathematical and Statistical Innovation, University of Chicago*, Chicago, IL, Feb. 25, 2025.
- [T10] “Towards Agent-based Autonomous Network Security,” at *IEEE COMSOC TCCN Rising Star Symposium Series, Stevens Institute of Technology*, Hoboken, NJ, Nov. 21, 2024.
- [T9] “Online Optimization Meets Urban Transportation,” at *C2SMARTER, Tier 1 University Transportation Center*, Brooklyn, NY, Nov. 8, 2024.
- [T8] “Conjectural Online Learning in Asymmetric Information Stochastic Games,” at *Systems Engineering Department Seminar, City University of Hong Kong*, HK, Oct. 7, 2024.
- [T7] “Agent of Agents: Meta LLM-Agent for Autonomous Security Operations,” at *NSF Workshop on Large Language Models for Network Security*, Brooklyn, NY, Oct. 2, 2024.
- [T6] “Conjectural Online Learning with First-order Beliefs in Asymmetric Information Stochastic Games,” at *Coordinated Science Laboratory, University of Illinois Urbana-Champaign*, Champaign, IL, Aug. 13, 2024.
- [T5] “Automated Security Response Through Conjectural Online Learning under Information Asymmetry,” at *Autonomous Robotics and Control Lab, California Institute of Technology*, Pasadena, CA, Jun. 21, 2024.
- [T4] “On the Role of Information Structures in Multi-agent Learning,” at *International Conference on Game Theory*, Stony Brook, NY, Jul. 21, 2022.
- [T3] “Informationally Mosaic Reinforcement Learning,” at *SIAM 2022 Annual Meeting Session on Markov Decision Processes*, Pittsburgh, PA, Jul. 12, 2022.
- [T2] “Correlated Learning over Networks,” at *INFORMS Annual Meeting Workshop on Multi-agent Learning*, Online, Nov. 16, 2020.
- [T1] “Directional Framelets and its Application in Medical Imaging,” at *PIMS-AMI Workshop on Applied Harmonic Analysis, University of Alberta*, Edmonton, Canada, Aug. 2017.

TEACHING & MENTORING

City University of Hong Kong

Sept. 2025 – Present

Undergraduate Teaching

- SYE2010 Fundamental Engineering Analysis and Design,

Fall 2025, Spring 2026

New York University

Sept. 2021 – May 2025

Graduate Teaching

- ECE-GY5213 Introduction to System Engineering, Teaching Assistant
- ECE-GY6263 Game Theory, Guest Lecturer
- ECE-GY6233 System Optimization Methods, Teaching Assistant

Fall 2023, Spring 2025

Fall 2022

Spring 2022

Graduate Mentoring

- Xinhong Xie, Current Position: Ph.D. student at Penn State University
Project: Large language models for personalized text detoxification
- Dhairya Upadhyay, Current Position: Data analyst at NYU Langone Health
Project: Vision-based turtlebot collision avoidance
- Haozhe Lei, Current Position: Ph.D. student at New York University
Project: Meta reinforcement learning for self-adaptive driving
- Nikunj Gupta, Current Position: Ph.D. student at the University of Southern California
Project: Informationally mosaic multi-agent reinforcement learning

Jan. 2024 – Sept. 2024

Jan. 2023 – May 2023

Sept. 2021 – May 2022

Sept. 2021 – Dec. 2021

Undergraduate Mentoring

- Junjie Huang, LLM-powered automated penetration testing and remediation
Best Student Paper Award at ACM CCS AutonomousCyber Wkshp 2024
- Juan Guevara, Self-confirming transformer in multi-agent reinforcement learning

Jun. 2024 – Sept. 2024

Jun. 2023 – Sept. 2023

PROFESSIONAL SERVICES & ACTIVITIES

Conference Organization

General Chair

- IEEE Control Systems Society Security and Privacy Rising Star Symposium, virtual, Sept. 2025
- NSF Workshop on LLMs for Network Security, Brooklyn, NY, Oct. 2024
- American Control Conference (ACC 2024), Workshop on Security and Privacy of the Next-Generation Cyber-Physical Systems, Toronto, Canada, Jul. 2024

Program Chair

- IEEE Conference on Communications and Network Security (CNS 2024), Cyber Resilience Workshop, Taipei, Taiwan, Oct. 2024
- IEEE Conference on Communications and Network Security (CNS 2023), Cyber Resilience Workshop, Orlando, FL, Oct. 2023

Publicity Chair

- The 2nd International Workshop on Autonomous Cybersecurity (AutonomousCyber 2025), in conjunction with the 30th European Symposium on Research in Computer Security (ESORICS), Toulouse, France, Sept. 2025
- IEEE International Conference on Computer Communications (INFOCOM 2025), Workshop on Resilience in Next-Generation Networks, London, UK, May 2025

Session Chair

- INFORMS Annual Meeting, Atlanta, GA, Oct. 2025
- Conference on Game Theory and AI for Security, Pittsburgh, PA, Oct. 2022
- SIAM Annual Meeting, Pittsburgh, PA, Jul. 2022
- International Conference on Game Theory, Stony Brook, NY, Jul. 2022

Technical Program Committee

- The 40th Annual AAAI Conference on Artificial Intelligence, Special Track on AI Alignment, Singapore, Jan. 2026
- The 8th AAAI/ACM Conference on AI, Ethics, and Society (AIES 2025), Madrid, Spain, Oct. 2025
- Workshop on Quantum Computing Security, Privacy, and Resilience, in conjunction with IEEE Quantum Week, Albuquerque, NM, Sept. 2025
- The 2nd International Workshop on Autonomous Cybersecurity (AutonomousCyber 2025), in conjunction with the 30th European Symposium on Research in Computer Security (ESORICS), Toulouse, France, Sept. 2025

Review Services

Journals

- IEEE Robotics and Automation Letters
- IEEE Control System Letters
- IEEE Transactions on Intelligent Transportation Systems
- IEEE Transactions on Emerging Topics in Computational Intelligence
- Nonlinear Analysis: Hybrid Systems
- Expert Systems with Applications
- Reliability Engineering & System Safety
- Journal of Cybersecurity

Conferences

- AAAI/ACM Conference on AI, Ethics, and Society (AIES2025)
- IEEE International Conference on Computer Communications (INFOCOM2025)
- IEEE Conference on Communications and Network Security (CNS2024/23)
- IEEE International Conference on Robotics Automation (ICRA2024/23)
- IEEE Conference on Decision and Control (CDC2025/24/23/22/21)
- Annual Learning for Dynamics & Control Conference (L4DC2023)
- International Joint Conferences on Artificial Intelligence (IJCAI2022)
- International Conference on Machine Learning (ICML2022)