Tao Li

370 Jay Street, Brooklyn, NY, 11201 | taoli@nyu.edu | https://taoli-nyu.github.io/

Education

New York University Brooklyn, NY
Ph.D. in Electrical Engineering *Sept. 2018 – May 2025*

- Dissertation: Multi-Agent Reinforcement Learning for Autonomous and Resilient Operations in Cyber-Physical-Human Networks.
- Advisor: Prof. Quanyan Zhu
- Awards: Dante Youla Award for Research Excellence 2024

Xiamen University Fujian, China
B.S. in Mathematics *Sept. 2014 – Jun. 2018*

- Awards: National Scholarship by Ministry of Education of China

Experience

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
Associate Director of NYU LARX Lab, Affiliate Member, NYU Center for Cybersecurity *Sept. 2020 – Oct. 2024*

Research Interests

- Theory: Reinforcement Learning, Game Theory, Control and Optimization, Operations Research.
- Applications: AI Security, Cybersecurity, Misinformation Detection & Mitigation, Autonomous Mobility, Robotics.

Publications

* *indicates equal contribution.*

Book Chapters

[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.

[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*, Springer Cham, 2024.

Journals

[J1] 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 intelligent mobility analytics for urban transportation management,” *IEEE Transactions on Intelligent Transportation Systems*, 2024, to appear.

[J2] 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*, 2024, to appear.

[J3] 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.

[J5] 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.

[J6] 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.

[J7] 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

[C1] 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 2024)*, Milan, Italy, Dec. 2024.

[C2] 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 2024)*, Milan, Italy, Dec. 2024.

[C3] 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 2024)*, Yokohama, Japan, May 2024.

[C4] 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, Hawaii, USA, Jul. 2023.

[C5] 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 2023)*, Singapore, Dec. 2023.

[C6] 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 2023)*, 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 2023)*, Singapore, Aug. 2023.

[C8] 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.

[C9] Y. Pan, T. Li, and Q. Zhu, "On the resilience of traffic networks under non-equilibrium learning," in *American Control Conference (ACC 2023)*, San Diego, CA, USA, May 2023.

[C10] 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 2023)*, London, United Kingdom, May 2023.

[C11] G. Peng, T. Li, S. Liu, J. Chen, and Q. Zhu, "Locally-aware constrained games on networks," in *American Control Conference (ACC 2021)*, virtual, May 2021.

[C12] T. Li, G. Peng and Q. Zhu, "Blackwell online learning for Markov decision processes," in *55th Annual Conference on Information Sciences and Systems (CISS 2021)*, virtual, Mar. 2021.

[C13] 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.

Working Papers

[W1] 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.

[W2] Y-T. Yang, T. Li, and Q. Zhu, "Transparent tagging for strategic social nudges on user-generated misinformation," submitted to *IEEE Transactions on Control of Network Systems*, 2024.

[W3] 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," submitted to *IEEE Open Journal of the Communications Society*, 2024.

[W4] X. Xie, T. Li, and Q. Zhu, “Learning from response not preference: A Stackelberg approach for LLM detoxification using non-parallel data,” arXiv preprint, 2024, arXiv: 2410.20298.

[W5] T. Li, J. Guevara, X. Xie, and Q. Zhu, “Self-confirming transformer for locally consistent online adaptation in multi-agent reinforcement learning,” arXiv preprint, 2023, arXiv: 2310.04579.

[W6] T. Li and Q. Zhu, “Commitment with signaling under double-sided information asymmetry,” arXiv preprint, 2022, arXiv:2212.11446.

[W7] T. Li, H. Lei and Q. Zhu, “Sampling attacks on meta reinforcement learning: A minimax formulation and complexity analysis,” arXiv preprint, 2021, arxiv:2208.00081.

[W8] 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.

Research Grants Experience

[G1] “Understanding Misperceptions of Cyber Risks to Model and Secure Transportation Infrastructures,” National Science Foundation, Program: SAI, PI: Quanyan Zhu, Status: *Awarded*, Amount: $309,890, Role: participated in proposal writing, Sept. 2021.

[G2] “Conference: Workshop on Large Language Models for Network Security,” National Science Foundation, Program: SaTC, PI: Quanyan Zhu, Status: *Awarded*, Amount: $50,000, Role: participated in proposal writing, Apr. 2024.

[G3] “Symbiotic Game and Large Language Models for Agent-Based Cyber Deception Operations,” Cisco Research, PI: Quanyan Zhu, Status: *Submitted*, Role: participated in proposal writing, Oct. 2024.

Invited Talks

[T1] “Towards Agent-based Autonomous Network Security,” at *IEEE COMSOC TCCN Rising Star Symposium Series, Stevens Institute of Technology*, NJ, Nov. 21, 2024.

[T2] “Online Optimization Meets Urban Transportation,” at *C2SMARTER, Tier 1 University Transportation Center*, NY, Nov. 8, 2024.

[T3] “Conjectural Online Learning in Asymmetric Information Stochastic Games,” at *Systems Engineering Department Seminar, CityU of Hongkong*, HK, Oct. 7, 2024.

[T4] “Agent of Agents: Meta LLM-Agent for Autonomous Security Operations,” at *NSF Workshop on Large Language Models for Network Security*, NY, Oct. 2, 2024.

[T5] “Conjectural Online Learning with First-order Beliefs in Asymmetric Information Stochastic Games,” at *Coordinated Science Laboratory, University of Illinois Urbana-Champaign*, IL, Aug. 13, 2024.

[T6] “Automated Security Response Through Conjectural Online Learning under Information Asymmetry,” at *Autonomous Robotics and Control Lab, California Institute of Technology*, CA, Jun. 21, 2024.

[T7] “On the Role of Information Structures in Multi-agent Learning,” at *International Conference on Game Theory*, Stony Brook, NY, Jul. 21, 2022.

[T8] “Informationally Mosaic Reinforcement Learning,” at *SIAM 2022 Annual Meeting Session on Markov Decision Processes*, Pittsburgh, PA, Jul. 12, 2022.

[T9] “Correlated Learning over Networks,” at *INFORMS Annual Meeting Workshop on Multi-agent Learning*, Online, Nov. 16, 2020.

[T10] “Directional Framelets and its Application in Medical Imaging,” at *PIMS-AMI Workshop on Applied Harmonic Analysis, University of Alberta*, Canada, Aug. 2017.

Awards

Rising Star in AI and Machine Learning in Security *2024*

- Awarded by IEEE TCCN 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 und2017ergrad research.

National Scholarship *2015*
- Awarded by the Ministry of Education of China for undergrad academic excellence.

Teaching & Mentoring

Graduate Teaching
- ECE-GY5213 Introduction to System Engineering, Teaching Assistant *Fall 2023*
- ECE-GY6263 Game Theory, Guest Lecturer *Fall 2022*
- ECE-GY6233 System Optimization Methods, Teaching Assistant *Spring 2022*

Graduate Mentoring
- Xinhong Xie, Current Position: Ph.D. student at Penn State University
  Project: Large language models for personalized text detoxification *Jan. 2024 – Sept. 2024*
- Dhairya Upadhyay, Current Position: Data analyst at NYU Langone Health
  Project: Vision-based turtlebot collision avoidance *Jan. 2023 – May 2023*
- Haozhe Lei, Current Position: Ph.D. student at New York University
  Project: Meta reinforcement learning for self-adaptive driving *Sept. 2021 – May 2022*
- Nikunj Gupta, Current Position: Ph.D. student at the University of Southern California
  Project: Informationally mosaic multi-agent reinforcement learning *Sept. 2021 –Dec. 2021*

Undergraduate Mentoring
- Junjie Huang, LLM-powered automated penetration testing and remediation
  Best Student Paper Award at ACM CSS AutonomousCyber Wkshp 2024 *Jun. 2024 – Sept. 2024*
- Juan Guevara, Self-confirming transformer in multi-agent reinforcement learning *Jun. 2023 – Sept. 2023*

Professional Services & Activities

Conference Organization
- General Chair for NSF Workshop on LLMs for Network Security, Brooklyn, NY, Oct. 2024.
- Technical Program Chair for IEEE Conference on Communications and Network Security (CNS 2024), Cyber Resilience Workshop, Taipei, Taiwan, Oct. 2024.
- Technical Program Chair for IEEE Conference on Communications and Network Security (CNS 2023), Cyber Resilience Workshop, Orlando, FL, Oct. 2023.
- Session Chair for SIAM Annual Meeting, Pittsburgh, PA, Jul. 2022.
- Session Chair for International Conference on Game Theory, Stony Brook, NY, Jul. 2022.

Review Services
- IEEE Robotics and Automation Letters
- IEEE Control System Letters
- IEEE Transactions on Emerging Topics in Computational Intelligence
- Nonlinear Analysis: Hybrid Systems
- IEEE Conference on Communications and Network Security (CNS-24/23)
- IEEE International Conference on Robotics Automation (ICRA-24/23)
- IEEE Conference on Decision and Control (CDC-24/23/22/21)
- Annual Learning for Dynamics & Control Conference (L4DC-23)
- International Joint Conferences on Artificial Intelligence (IJCAI-22)
- International Conference on Machine Learning (ICML-22)

References

- Dr. Quanyan Zhu, Associate Professor, Department of Electrical and Computer Engineering & Center for Cybersecurity, New York University, 370 Jay Street, Brooklyn, NY, 11201, qz494@nyu.edu, Phone: 646-997-3371
- Dr. Sundeep Rangan, Professor, Department of Electrical and Computer Engineering & Director of Wireless Center, New York University, 370 Jay Street, Brooklyn, NY, 11201, srangan@nyu.edu, Phone: 646-997-3804
- Dr. Kaan Ozbay, Professor, Department of Civil and Urban Engineering and Center for Urban Science and Progress & Founding Director of C2SMART Center, New York University, 6 MetroTech Center, 4th Floor, RH 441, Brooklyn, NY 11201, kaan.ozbay@nyu.edu, Phone: 646-997-2691
- Dr. Tamer Başar, Swanlund Endowed Chair Emeritus & Center for Advanced Study Professor Emeritus, Department of Electrical and Computer Engineering, University of Illinois Urbana-Champaign, Coordinated Science Laboratory, University of Illinois, 1308 West Main, Urbana, IL 61801, basar1@illinois.edu, Phone: 217-979-1283

Last updated on December 8, 2024