KAIYUAN TAN

kaiyuan.t@wustl.edu scholar.google.com/kaiyuan tankevin.github.io

BIOGRAPHY

I am currently a **Ph.D. student** at the Department of Computer Science, **Vanderbilt University**. My research goal is to build a safe and robust cyber-physical system. My recent work focuses on optimization-based adversarial attacks and learning-enabled control and planning.

Research Interests: Physics-informed Machine Learning, Adversarial Attack, Optimization

EDUCATION

Ph.D. in Computer Science Jan 2024 - Current
Vanderbilt University, TN, USA
Advisor: Dr. Thomas Beckers
Research Focus: "Physics-informed Machine Learning"

M.S. in Electrical Engineering Aug 2021 - May 2023
Washington University in St. Louis, St. Louis, MO, USA
Advisor: Dr. Yiannis Kantaros
Thesis: "Targeted Adversarial Attack Generation and Detection"

B.Eng. in Information Engineering Aug 2017 - May 2021
Sun Yat-Sen University, Guangzhou, Guangdong, China
Advisor: Dr. Lei Sun
Thesis: "Estimation of mixed noise parameters depending on hyperspectral images signals"

WORK EXPERIENCE

Research Associate Student (Robotics & Learning-Enabled Control) Aug 2023 - Current
Vanderbilt University, Nashville, TN, USA
Advisor: Dr. Thomas Beckers

Research Associate Intern (Robotics & Cyber-Physical System Security) May 2023 - July 2023
Washington University in St. Louis, St. Louis, MO, USA
Advisor: Dr. Ning Zhang

Research Associate Student (Adversarial Attack & Learning-Enabled Control) June 2022 - May 2023
Washington University in St. Louis, St. Louis, MO, USA
Advisor: Dr. Yiannis Kantaros

PUBLICATIONS

[1] **K. Tan**, P. Li, and T. Beckers, "Physics-Constrained Learning of PDE Systems with Uncertainty Quantified Port-Hamiltonian Models." 6th Annual Learning for Dynamics & Control Conference at Oxford (**L4DC**), 2024.

[2] **K. Tan**, J. Wang, and Y. Kantaros, "Targeted Adversarial Attacks against Neural Network Trajectory Predictors." 5th Annual Learning for Dynamics & Control Conference at UPenn (**L4DC**), 2023.

[3] **K. Tan**, Z. Wang, Z. Liu, and L. Sun, "Research on Full-Space Spectrum-Sharing Strategy for Massive MIMO Cognitive Radio Systems" The 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), (pp. 639-644). IEEE.

PRE-PRINTS

[1] J. Wang, Jiaming Tong, **K. Tan**, and Y. Kantaros, “Large Language Model Based Robot Planning with Safety-Guaranteed Temporal Logic Task Specification.”

[2] J. Wang, **K. Tan**, Z. Sun, and Y. Kantaros, “Mission-driven Exploration for Accelerated Deep Reinforcement Learning with Temporal Logic Task Specifications.”

TECHNICAL SKILLS

Programming Languages Python, Matlab, C/C++
Deep Learning Frameworks Pytorch

AWARDS

S Award, US Mathematical Contest in Modeling, 2018-2019.