KAIYUAN TAN

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

BIOGRAPHY

I am currently a **Research Associate** 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: Adversarial Attack, Cyber-Physical System, Optimization, Machine Learning

EDUCATION

M.S. in Electrical Engineering Aug 2021 - May 2023
Washington University in St. Louis, St. Louis, MO, USA GPA: 3.45/4.0
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 Extrodinary Class
Advisor: Dr. Lei Sun
Thesis: "Estimation of mixed noise parameters depending on hyperspectral images signals"

WORK EXPERIENCE

Research Associate Intern (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] J. Wang, Jiaming Tong, **K. Tan**, and Y. Kantaros, "Large Language Model Based Robot Planning with Safety-Guaranteed Temporal Logic Task Specification." in the 2024 IEEE International Conference on Robotics and Automation (**ICRA** 2024). (Under Reviewing)

[2] J. Wang, **K. Tan**, Z. Sun, and Y. Kantaros, "Mission-driven Exploration for Accelerated Deep Reinforcement Learning with Temporal Logic Task Specifications." in the 2024 IEEE International Conference on Robotics and Automation (**ICRA** 2024). (Under Reviewing)

[3] **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.

[4] **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.

RESEARCH EXPERIENCE

- **Accelerated Deep Reinforcement Learning with Temporal Logic Task Specifications (WashU)**
  Advisor: Assistant Prof. Yiannis Kantaros Dec 2022 - Feb 2023
  - Developed a novel accelerated reinforcement learning algorithm for mobile robots, incorporating mission and safety requirements specified using Linear Temporal Logic (LTL) [2].
  - Collaborated on the creation of an approach that significantly outperforms baseline and related methods in learning control policies, and conducted real-world testing. The paper has been **submitted** to in the 2024 IEEE International Conference on Robotics and Automation (**ICRA** 2024).
- **Targeted Adversarial Attacks against Neural Networks for Trajectory Prediction Tasks (WashU)**
  Advisor: Assistant Prof. Yiannis Kantaros Aug 2022 - Dec 2022
  - Developed the first targeted adversarial attack, TA4TP[3], against Deep Neural Network models used for trajectory prediction tasks.
  - Implemented the code efficiently generates adversarial input examples, causing the DNN model to predict desired trajectories that can lead to a collision or forced stop of the victim's vehicle non-invasively. The paper has been **published** on the 5th Annual Learning for Dynamics & Control Conference (**L4DC**).
- **Research on Full-Space Spectrum-Sharing Strategy for Massive MIMO Cognitive Radio Systems(SYSU)**
  Advisor: Associate Prof. Lei Sun Jun 2020 - Dec 2020
  - Gave a new greedy-oriented method to perform the optimization in cognitive radio resource allocation using angular information[4].
  - Built the model and wireless channel estimation via Matlab; the paper was **published** on the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering 2021(ICCECE), and it currently has **two citations**.
- **Estimation of mixed noise parameters depending on hyperspectral images signals(SYSU)**
  Advisor: Associate Prof. Lei Sun Dec 2020 - Apr 2021
  - Solved the inverse problem on high-dimensional image processing. Estimated the parameters of a mixture of signal-independent and signal-dependent noises in hyperspectral images
  - Drafted the integrated high-dimensional image processing procedure, including downsampling, segmentation, and clustering; the outcomes were used as my **bachelor thesis**.
- **Automated Fundus Diseases Detection from SD-OCT and IR Using Multimodal Deep Learning Approach(SYSU)**
  Advisor: Assistant Prof. Shanshan Liang Jun 2020 - Jun 2021
  - Designed and proposed six parallel dense sparse attention bimodal fusion CNN models with parallel complementary structures to simultaneously use fundus infrared photography (IR) and fundus OCT images to detect common fundus retinal diseases
  - Established the first-hand database for image feature extraction cooperating with Zhongshan Eye State Key Lab. And we used various neural networks, such as VGG16, Resnet, Se-Resnet, to compare the accuracy.

TECHNICAL SKILLS

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

AWARDS

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