WENDA CHU

chuwd19@mails.tsinghua.edu.cn
+86 13510119658 Homepage
Shenzhen, Guangdong, China, 518067

EDUCATION

Tsinghua University, Beijing, China — *September 2019 - July 2023 (expected)*
Bachelor of Computer Science, Yao Class, IIIS — **Overall GPA: 3.88 (transcript)**

PUBLICATIONS

TPC: Transformation-Specific Smoothing for Point Cloud Models Paper
Authors: **Wenda Chu**, Linyi Li, Bo Li — Preprint, under review.

RESEARCH EXPERIENCE

Provable Defense for point cloud models — University of Illinois, Urbana Champaign
Mentor: Bo Li — *October 2021-present*

- Proposed a transformation specific smoothing framework for point cloud models that yields provable robustness against a various class of semantic transformations, which significantly boosts the certified accuracy under perturbations (e.g., 20.3% to 83.8% for twisting in $\pm 20°$).
- Showed the scalability of our proposed framework to larger point clouds, which implies its capability of dealing with real-world scenarios, such as LiDAR-based object detection for autonomous driving systems.

Physical world attacks on object detection algorithms — Tsinghua University
Mentor: Xiaolin Hu — *June 2021-present*

- Designed a pipeline that attacked object detection models in three dimensional physical world by T-shirts textures in two dimensional digital space, in which figures of human wearing the T-shirts were rendered using differentiable functions and were randomly transformed to simulate photos taken in the real world.
- Derived T-shirt textures in camouflage patterns that evade both visual observation of eyes and object detection of algorithms from any direction. (See My Notes on Adversarial Machine Learning.)

SELECTED COURSE PROJECTS

Traffic at Peak Hours: A Game Theory View Paper Code

- Modeled the unusual concentration of passengers on one direction of the subway during peak hours as a game and analyzed the detouring actions of passengers that they travel in the reverse direction to assure getting on train.
- The result showed how excessive competition on limited resources such as transportation may cause a huge decrease on social welfare.

A Survey on Differential Privacy Paper

- Surveyed over differential privacy algorithms and their applications.
- Gained insights into the power of randomness towards provable security.

Diversifying Options in Option-Critic Framework of Hierarchical Reinforcement Learning Paper

- Implemented Option-Critic architecture and reproduced its result on maze problems
- Introduced intrinsic rewards to option level and enhanced option specialization on termination probability.
- Our methods diversified the options in the higher level of hierarchical reinforcement learning.

SKILLS

Programming Skills: Python, PyTorch (proficient), C, C++, Go, SQL, MATLAB, Verilog, LaTeX.
Language Skills: Chinese(native), English(TOEFL 111: R30 L30 S24 W27).
GRE: Verbal Resoning 159, Quantitative Reasoning 169, Analytical Writing 4.0.

HONORS AND AWARDS

- **2nd** place in the 35th Chinese Physics Olympiad (CPhO) 2018
- Scholarship for Freshmen - Tsinghua University 2019
- Sports Excellence Award - Tsinghua University 2020
- Sports Excellence Award - Tsinghua University 2021