WENDA CHU

+86 13510119658 Homepage
chuwd19@mails.tsinghua.edu.cn

RESEARCH INTEREST

My research interests lie primarily in the **theory of machine learning**, especially in **federated learning**, **optimization**, and the **robustness**, **safety**, and **fairness** aspects of machine learning.

EDUCATION

Tsinghua University, Beijing, China — *September 2019 - July 2023 (expected)*
Bachelor of Computer Science, Yao Class, IIIS — **Overall GPA: 3.90/4.00 (transcript)**

PUBLICATIONS

TPC: Transformation-Specific Smoothing for Point Cloud Models Paper
Authors: **Wenda Chu**, Linyi Li, Bo Li ICML 2022.

FOCUS: Fairness via Agent-Awareness for Federated Learning on Heterogeneous Data Paper.
Authors: **Wenda Chu***, Chulin Xie*, Boxin Wang, Linyi Li, Lang Yin, Han Zhao, Bo Li Under Review.

Physically Realizable Natural-Looking Clothing Textures Evade Person Detectors via 3D Modeling
Authors: Zhanhao Hu*, **Wenda Chu***, Xiaopei Zhu, Hui Zhang, Bo Zhang, Xiaolin Hu Under Review.

COMMIT: Certifying Robustness of Multi-Sensor Fusion Systems against Semantic Attacks
Authors: Zijian Huang*, **Wenda Chu***, Linyi Li*, Chejian Xu, Bo Li Under Review.

PerAda: Parameter-Efficient and Generalizable Federated Learning Personalization with Guarantees Under Review
Authors: Chulin Xie, De-An Huang, **Wenda Chu**, Daguang Xu, Chaowei Xiao, Bo Li, Anima Anandkumar

RESEARCH EXPERIENCE

Certifiable Robustness for Point Cloud Models — University of Illinois, Urbana Champaign
Advisor: Bo Li — *October 2021-January 2022*

- Proposed a transformation-specific smoothing framework for point cloud models to provide **certifiable robustness** against a wide range of semantic transformations.
- Provided a taxonomy for transformations on point cloud models according to their closure property and proposed a concrete certification protocol for each.
- Our TPC method significantly **boosts the certified robust accuracy** under perturbations (e.g., 20.3% to 83.8% for twisting in ±20°).

Fair Federated Learning on Heterogeneous Data — University of Illinois, Urbana Champaign
Advisor: Bo Li, Han Zhao — *February 2022-May 2022*

- Defined a fairness metric for federated learning via agent-awareness (FAA) based on the excess risks by recognizing the **heterogeneous contribution** of clients.
- Proposed a fair FL algorithm based on agent clustering (FOCUS) to improve fairness measured by FAA, especially in the non-IID data settings. We proved the **linear convergence rate** and **optimality** of FOCUS under linear models and general convex losses.

- Proved that FOCUS achieves **stronger fairness** in terms of FAA compared with FedAvg on both linear models and general convex losses regarding outlier agents.
- Showed that FOCUS empirically achieves significantly higher fairness in terms of FAA while maintaining similar or even higher prediction accuracy compared with FedAvg and other existing fair FL algorithms.

Physical World Attacks on Object Detection Algorithms Tsinghua University
Advisor: Xiaolin Hu *June 2021-January 2022*

- Devised a pipeline that attacked object detection models in the physical world from any viewing angle by adversarial clothes.
- Proposed a differentiable process for generating natural adversarial textures using Voronoi diagrams. To mitigate the gap from digital space to the physical world, we proposed a non-rigid mesh augmentation algorithm using topologically plausible projection.

Distributed Differentially Private Generative Models University of Illinois, Urbana Champaign
Advisor: Bo Li *July 2022-Present*

- Considered the problem of training **differentially private generative models** with **distributed** and **heterogeneous** datasets. We explained why previous algorithms fail when remote datasets are heterogeneous by analyzing its Nash equilibrium.
- Proposed a private distributed GAN framework with discriminators distributed on remote clients. The gradients from discriminators are clustered iteratively using an EM algorithm and privately aggregated to train generators on the central server.
- Showed how clustering helps boost the model performance for non-IID distributed data under strict privacy constraints. Our work is planned for ICML 2023.

Certifiable Robustness for Multi-sensor Fusion Systems University of Illinois, Urbana Champaign
Advisor: Bo Li *February 2022-Present*

- Presented a general framework for certifying the robustness of multi-sensor fusion systems for object detection against common transformations. We proved theorems for certified lower bounds for IoU of 3D bounding boxes.
- Evaluated our method on simulation environments for autonomous driving. We plan to submit our work to ICML 2023.

SELECTED COURSE PROJECTS

Distributed Robust Principal Component Analysis Paper

- Proposed the first distributed RPCA algorithm based on matrix factorization with consensus.
- Theoretically proved the convergence of our algorithm and numerically analyzed its performance on synthetic data.

A Survey on Differential Privacy Paper

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

SKILLS

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

HONORS AND AWARDS

- Scientific Innovation Excellence Award - Tsinghua University 2022
- Sports Excellence Award - Tsinghua University 2021
- Sports Excellence Award - Tsinghua University 2020
- Scholarship for Freshmen - Tsinghua University 2019
- **2nd** place in the 35th Chinese Physics Olympiad (CPhO) 2018