Jingkang Wang

www.cs.toronto.edu/~wangjk/

Email : wangjk@cs.toronto.edu
Mobile : (437) 985-0337

Research Interests

- **Machine Learning, Computer Vision, Trustworthy ML**

Education

- **University of Toronto** — Ontario, Canada
  Ph.D. in Computer Science (Direct Entry) — *Sept 2019 – Aug 2024 (Expected)*
  - **Advisors:**: Professors Raquel Urtasun and Richard Zemel
- **Shanghai Jiao Tong University (SJTU)** — Shanghai, China
  B.S. in Information Security — *Sept 2015 – June 2019*
  - **GPA**: 4.00/4.3 (91.8/100) **Rank**: 2/97

Research Internships

- **Ant Financial, Alibaba Group** — Zhejiang, China
  Research Intern (Algorithm Engineer Intern) — *June 2019 – July 2019*
  - **Advisor**: Professor Le Song
  - **Research Focus**: Adversarial Machine Learning
- **University of Illinois Urbana-Champaign (UIUC)** — Illinois, USA*
  Research Intern, Computer Science Department — *June 2018 – Oct 2018*
  - **Advisors**: Professors Bo Li
  - **Research Focus**: Robust Reinforcement Learning

Publications or Manuscripts

- **Beyond Adversarial Training: Min-Max Optimization in Adversarial Attack and Defense** **[pdf]**
  Jingkang Wang*, Tianyun Zhang*, Sijia Liu, Pin-Yu Chen, Jiacen Xu, Makan Fardad and Bo Li.
- **Reinforcement Learning with Perturbed Rewards** **[pdf]**
  Jingkang Wang, Yang Liu and Bo Li.
- **An Information-Theoretic Perspective on Adversarial Vulnerability**
  Ruoxi Jia, **Jingkang Wang**, Bo Li and Dawn Song.
- **Multiple Character Embeddings for Chinese Word Segmentation** **[pdf]**
  Jingkang Wang*, Jianing Zhou*, Jie Zhou and Gongshen Liu.
  In Proceedings of 57th Annual Meeting of the ACL, Student Reseach Workshop, 2019
- **LiDAR-Video Driving Dataset: Learning Driving Policies Effectively** **[pdf]**
  Yiping Chen*, **Jingkang Wang***, Jonathan Li, Cewu Lu, Zhipeng Luo, Han Xue and Cheng Wang.
  In Proceedings of IEEE Conference on CVPR, 2018

Research Experience

- **Min-Max Optimization in Adversarial Machine Learning** — *July 2018 - Oct. 2018*
  - ***Advisor:*** *Profs. Sijia Liu and Bo Li*
  - Propose a general and theoretically grounded min-max framework on adversarial attack and defense.
  - Re-formulate many problem set-ups under proposed framework including attacking model ensemble, devising robust perturbation over multiple images or transformations, adversarial training under mixed types of attacks.
  - Provide a holistic tool for self-risk assessment by learning domain weights.
- **Reinforcement Learning with Perturbed Rewards** — *Feb 2019 - June 2019*
  - ***Advisor:*** *Profs. Yang Liu and Bo Li*
  - Introduce an unbiased estimator of reward in reinforcement learning which guarantees risk minimization without any assumptions on the true distribution.
  - Propose an efficient iterative algorithm for estimating the confusion matrices of corrupted rewards in the training.
  - Study the convergence and finite sample complexity theoretically under the proposed reward proxy.
- **Understanding Adversarial Examples as the Abuse of Redundancy** — *Mar 2018 - July 2018*
  - ***Advisor:*** *Profs. Bo Li and Dawn Song*

- Propose a model for adversarial examples consistent with related work, physics and information theory.
- Reinterpret the Helmholtz free energy formula to explain the relationship between content and noise for sensor-based data.
- Prove that input redundancy is a necessary condition for being able to generate adversarial examples.
- Validate that adversarial examples are indeed overflowing perceptrons trained on a certain level of redundancy.

- **Multiple Embeddings for Chinese Word Segmentation** *Feb 2018 - May 2018*
  - ***Advisor:*** *Prof. Gongshen Liu*
  - Leverage both semantic and phonetic features of Chinese characters in NLP tasks by introducing *Pinyin Romanization* and *Wubi Input* Embeddings.
  - Achieve the state-of-the-art performance in AS and CityU corpora with F1 scores of 96.9 and 97.3.
- **Benchmark for Driving Policy Learning** *Apr 2017 - Feb 2018*
  - ***Advisor:*** *Prof. Cewu Lu*
  - Propose a dataset which is the first policy learning benchmark composed of driving videos, LiDAR data, and corresponding driving behaviors.
  - Conduct the complete analysis on how important depth information is, how to leverage depth information and what we can achieve by utilizing current techniques.

Honors & Awards

- **National Scholarships (*Top 0.2% Nationwide*)** *2016, 2017, 2018*
- **Level-A SJTU Outstanding Scholarships (*Top 1% in SJTU*)** *2016, 2017, 2018*
- **SenseTime Scholarship** *2018*
- **Yitu Technology Scholarship** *2017*
- **Excellent Bachelor Thesis (Top %1) of SJTU** *2019*
- **Outstanding Undergraduate in Shanghai** *2019*
- **SJTU Merit Students** *2016, 2017, 2018*

Competitions

- **First Prize in National College Student Information Security Contest** *2018*
- **Meritorious Winner Prize of Mathematical Contest in Modeling** *2018*
- **Second Prize in National College Student Information Security Contest** *2017*
- **Second Prize in The Chinese Mathematics Competitions (Shanghai)** *2017*
- **Third Prize in Parts of The National Physics Contest for College Students** *2016*
- **First Prize in Chinese Mathematical Olympiad (*10th in Province*)** *2014*

Interests & Skills

- **Hobbies**: Calligraphy, Violin, Badminton, Reading, Movie, Animation
- **Programming**: Python (Tensorflow, Pytorch), C++, LaTeX

Last Update: Aug 10, 2019

* indicates equal contribution (alphabetical order) or remote collaboration