Jingkang Wang

University of Toronto & Vector Institute
Department of Computer Science
Machine Learning Group

(+1) 437-985-0337
wangjk@cs.toronto.edu
www.cs.toronto.edu/~wangjk/

RESEARCH INTERESTS

- Automatic & Trustworthy Machine Learning
- Self-Driving - Training, Testing and Simulation
- 3D Computer Vision

EDUCATION

Ph.D. Student, **University of Toronto** Sep 2019 – present

- Department of Computer Science
- Advisor: Prof. Raquel Urtasun

B.S., Information Security, **Shanghai Jiao Tong University, China** Sep 2015 – Jun 2019

- GPA: 4.00/4.3 (91.8/100), **Rank: 1/97**
- Advisor: Prof. Cewu Lu

RESEARCH EXPERIENCE

Research Scientist, **UberATG Toronto**, Canada Sep 2019 – Feb 2021

- Manager: Prof. Raquel Urtasun
- Focus: Automating the Training & Testing for Self-Driving

Research Intern, **Ant Financial, Alibaba Group**, China Jun 2019 – Aug 2019

- Host: Prof. Le Song
- Focus: Decision-based Black-box Attack

Research Intern, **University of Illinois at Urbana-Champaign**, China (remotely) Oct 2018 – May 2019

- Host: Prof. Bo Li
- Focus: Trustworthy Machine Learning
- Work with Profs. Yang Liu (UCSC), Sijia Liu (MSU) and Ruoxi Jia (Virginia Tech)

Research Intern, **University of California, Berkeley**, China (remotely) Jun 2018 – Sep 2018

- Host: Prof. Bo Li and Prof. Dawn Song
- Focus: Trustworthy Machine Learning

PUBLICATIONS

Note: * below denotes equal contribution (co-first author). See Google Scholar.

CONFERENCES

[1] **Jingkang Wang**, Ava Pun, James Tu, Sivabalan Manivasagam, Abbas Sadat, Sergio Casas, Mengye Ren and Raquel Urtasun. AdvSim: Generating Safety-Critical Scenarios for Self-Driving Vehicles. *IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2021.*

[2] Nicholas Vadivelu, Mengye Ren, James Tu, **Jingkang Wang** and Raquel Urtasun. Learning to Communicate and Correct Pose Errors. *Conference on Robot Learning (**CoRL**), 2020.*

[3] **Jingkang Wang**, Yang Liu and Bo Li. Reinforcement Learning with Perturbed Rewards. *AAAI Conference on Artificial Intelligence (**AAAI**), 2020.* (**Spotlight**)

[4] Gerald Friedland, Ruoxi Jia, **Jingkang Wang**, Bo Li and Nathan Mundhenk. On the Impact of Perceptual Compression on Deep Learning. *International Conference on Multimedia Information Processing and Retrieval (**MIPR**), 2020.*

[5] **Jingkang Wang***, Jianing Zhou*, Jie Zhou and Gongshen Liu. Multiple Character Embeddings for Chinese Word Segmentation. *Annual Meeting of the Association for Computational Linguistics (**ACL**), 2019.*

[6] Yiping Chen*, **Jingkang Wang***, Jonathan Li, Cewu Lu, Zhipeng Luo, Han Xue and Cheng Wang. LiDAR-Video Driving Dataset: Learning Driving Policies Effectively. *IEEE Conference on Computer Vision and Pattern Recognition (**CVPR**), 2018.*

WORKSHOPS

[1] **Jingkang Wang***, Mengye Ren*****, Ilija Bogunovic, Yuwen Xiong and Raquel Urtasun. Cost-Efficient Online Hyperparameter Optimization. *International Conference on Machine Learning (**ICML**), RealML Workshop, 2020*.

[2] **Jingkang Wang***, Hongyi Guo*, Zhaowei Zhu and Yang Liu. Policy Learning Using Weak Supervision. *Advances in Neural Information Processing Systems (**NeurIPS**), DeepRL and RWRL Workshops, 2020*.

[3] **Jingkang Wang***, Gaoyuan Zhang* and Sijia Liu. Is Robust Neurons' Activation Sufficient to Robustify CNNs against Adversarial Attacks? *ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**), AdvML Workshop, 2020*.

[4] Tianshi Cao*, **Jingkang Wang***, Annie Zhang and Sivabalan Manivasagam. BabyAI++: Towards Grounded-Language Learning beyond Memorization. *International Conference on Learning Representations (**ICLR**), BeTR-RL Workshop, 2020*.

PREPRINT OR SUBMISSION

[1] James Tu*, Tsunhsuan Wang*, **Jingkang Wang**, Sivabalan Manivasagam, Mengye Ren and Raquel Urtasun. Adversarial Attacks on Multi-Agent Communication. *arXiv 2021*.

[2] **Jingkang Wang***, Tianyun Zhang*, Sijia Liu, Pin-Yu Chen, Jiacen Xu, Makan Fardad and Bo Li. Towards a Unified Min-Max Framework for Adversarial Exploration and Robustness. *arXiv 2019*.

SELECTED HONORS & AWARDS

- National Scholarships in China (**1%**), 2016, 2017, 2018
- Level-A SJTU Outstanding Scholarships (**1%**) 2016, 2017, 2018
- Excellent Bachelor Thesis (Top %1) of SJTU 2019
- Outstanding Undergraduate in Shanghai 2019
- First Prize in National College Student Information Security Contest 2018
- Meritorious Winner Prize in The Mathematical Contest in Modeling (MCM) 2018
- Second Prize in The Chinese Mathematics Competition (CMC, Shanghai) 2017
- Second Prize in National College Students Information Security Contest 2017
- First Prize in Chinese Mathematical Olympiad (CMO, **10th in Province**) 2014

PROFESSIONAL SERVICE

I am/was a reviewer for

- International Conference on Computer Vision (ICCV)
- IEEE Conference on Computer Vision and Pattern Recognition (CVPR)
- Annual Meeting of the Association for Computational Linguistics (ACL)
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)
- International Conference on Pervasive Artificial Intelligence (ICPAI)

TALKS & PRESENTATIONS

- On the Importance of Initialization and Momentum in Deep Learning. CSC2541. Mar 2021
- Physics-based Differentiable Rendering. UofT Reading Group. Mar 2021
- Differentiable Monte Carlo Ray Tracing through Edge Sampling. CSC2547. Feb 2021
- Trust Region Policy Optimization (TRPO). CSC2621. Feb 2020
- Efficient Nonmyopic Active Search. CSC2547 Learning to Search. Oct 2019
- Towards Secure and Interpretable Learning in Deep Neural Networks. Uber ATG. Jul 2019

[*CV updated on 2021-03-19.*]