TAO YU

Gates Hall G23, Cornell University, Ithaca, NY
Homepage: http://www.cs.cornell.edu/∼tyu/
Email: tyu@cs.cornell.edu

EDUCATION

Cornell University, Ithaca, NY, United States *Sep. 2019 - Present*
Ph.D. in Computer Science Dept. of Computer Science
Shanghai Jiao Tong University, Shanghai, China *Sep. 2015 - Jun. 2019*
B.S. in Mathematics and Applied Mathematics (Honors) ZhiYuan college

RESEARCH INTEREST

I am interested in robust and private machine learning. Some topics in this area that I am actively working on are defending against adversarial examples, developing privacy-preserving algorithms and mitigating the trade-off between accuracy and robustness & privacy (with applications in federated learning). Beyond this scope, I am also interested in adopting hyperbolic geometry in ML for stronger models.

PUBLICATIONS

Tao Yu, Eugene Bagdasaryan, Vitaly Shmatikov. "Salvaging Federated Learning by Local Adaptation" (Preprint).

Tao Yu, Christopher De Sa. "Numerically Accurate Hyperbolic Embeddings Using Tiling-Based Models". —In 33rd Conference on Neural Information Processing Systems (NeurIPS 2019). **Spotlight**.

Tao Yu*, Shengyuan Hu*, Chuan Guo, Weilun Chao, Kilian Q. Weinberger. "A New Defense Against Adversarial Images: Turning a Weakness into a Strength". —In 33rd Conference on Neural Information Processing Systems (NeurIPS 2019).

Felix Wu, Tianyi Zhang, Amauri Holanda de Souza Jr., Christopher Fifty, **Tao Yu**, Kilian Q. Weinberger. "Simplifying Graph Convolutional Networks". —In 36th International Conference on Machine Learning (ICML 2019).

Tao Yu, Huan long, John Hopcroft. "Curvature-based Comparison of Two Neural Networks". —In 24th International Conference on Pattern Recognition (ICPR 2018).

Tao Yu, Yu Qiao, Huan Long. "Knowledge-based Fully Convolutional Network and Its Application in Segmentation of Lung CT Images". (Technical Report).

Tao Yu, XiaoDong Zhang. "Structure of Graphs with Maximum Wiener Index". (Technical Report).

TALKS

NeurIPS 2019, "Numerically Accurate Hyperbolic Embeddings Using Tiling-Based Models".

EMPLOYMENT

Research Intern, Apple, remote work in USA. *June 1st 2020 - Aug. 21st 2020*
Manager: Ulfar Erlingsson Trui AI/ML Privacy Team, MLPT
— Worked with Ulfar on federated learning with privacy guarantees, in particular examine the privacy vulnerabilities in private federated learning, evaluate different privacy mechanisms (e.g. DP, SeparatedDP) with practical inference and reconstruction attacks.
— Proposed a new data poisoning attack to craft outliers and theoretically measure the lower bound of privacy leakage in federated learning.

Research Intern, Cornell University, Ithaca, NY, USA. *July. 2018 - Dec. 2018*
Supervisor: Kilian Q. Weinberger, Christopher De Sa Dept. of Computer Science
— Worked with Kilian on defending against adversarial examples. We proposed an algorithm to detect white-box adversarial attacks efficiently and accurately based on boundary information. Our result is submitted and accepted to NeurIPS 2019.
— Worked with Kilian on simplifing graph convolution networks. We proposed the SGC model to speed up training with comparable performances to graph convolutional networks on a variety of tasks. Our result is submitted and accepted to ICML 2019.
— Worked with Chris on the precision problem of hyperbolic embeddings, we constructed a better representation of hyperbolic space, which can represent any point within a constant distance (provably). Empirically our model outperforms state-of-the-art results. Our result is submitted and accepted to NeurIPS 2019 as a spotlight.

Research Intern, MSAR, BeiJing, CHINA. *March. 2019*
Supervisor: Jifeng Dai Visual Computing
— Empirically studied the spatial attention mechanism in different scenarios, in particular, the graph attention networks, we found that previous attention mechanism is redundant and not efficient, so we proposed a more efficient attention mechanism in graph networks.

HONORS & AWARDS

Excellent Students Scholarship in University, SJTU *2018,2017,2016,2015*
ZhiYuan Honors Scholarship, SJTU *2017,2016*
First Class Award in The Pan-Pearl River Delta and Chinese Elite Schools Physics Olympiad *2014*
Second Prize in Chinese Mathematical Olympiad in High School *2014*
Second Prize in Chinese Physics Olympiad *2014*

SKILLS & INTERESTS

Programming: Proficient in Python, C++, Mathematica, LaTex
Frame: Pytorch, Tensorflow, Caffe, Keras

EXTRACURRICULAR ACTIVITY

Debate Team, Core member *Sep. 2015 - June 2016*
Trained and participated in debate competitions in college and university.
Chairperson of Ace Offer - Freshman Cup Debate.
Social Practice Team, leader *June 2016 - July 2016*
Organize social practices: research of Nanjing regional culture, gain experience in managing, training, motivating teammates and serving society.
Detective Association of SJTU, Minister *Feb. 2017 - July 2018*
Actively participate in the management and planning activities, make outstanding contributions to the development of the association.
Volunteer Activities *Apr. 2016, Oct. 2016*
Volunteer in Shanghai international marathon and Shanghai international half marathon (Chinese athletics association).
Volunteer in Shanghai young physicists' tournament (Shanghai physical society)