Kevin Yuanshun Yao

ysyao@cs.uchicago.edu
https://people.cs.uchicago.edu/~ysyao

Education

09/2017-06/2020	**University of Chicago** Ph.D. in Computer Science Advisor: Prof. Ben Y. Zhao and Prof. Heather Zheng	Chicago, IL
09/2015-06/2017	**University of California, Santa Barbara** Ph.D. in Computer Science (transferred to UChicago)	Santa Barbara, CA
09/2011-05/2015	**University of Minnesota – Twin Cities** B.S. in Computer Science, Mathematics, and Statistics Research Advisor: Prof. Vipin Kumar	Minneapolis, MN

Publications

[1] **Yuanshun Yao**, Huiying Li, Haitao Zheng and Ben Y. Zhao. "Latent Backdoor Attacks on Deep Neural Networks." Proceedings of *ACM Conference on Computer and Communications Security* (**CCS**), London, UK, November 2019.

[2] Bolun Wang, **Yuanshun Yao**, Shawn Shan, Huiying Li, Bimal Viswanath, Haitao Zheng and Ben Y. Zhao. "Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks." Proceedings of *IEEE Symposium on Security and Privacy* (**IEEE S&P**), San Francisco, CA, May 2019.

[3] Bolun Wang, **Yuanshun Yao**, Bimal Viswanath, Haitao Zheng and Ben Y. Zhao. "With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning." Proceedings of *USENIX Security Symposium* (**USENIX Security**), Baltimore, MD, August 2018.

[4] **Yuanshun Yao**, Zhujun Xiao, Bolun Wang, Bimal Viswanath, Haitao Zheng and Ben Y. Zhao. "Complexity vs. Performance: Empirical Analysis of Machine Learning as a Service." Proceedings of *ACM SIGCOMM Internet Measurement Conference* (**IMC**), London, UK, November 2017.

[5] **Yuanshun Yao**, Bimal Viswanath, Jenna Cryan, Haitao Zheng and Ben Y. Zhao. "Automated Crowdturfing Attacks and Defenses in Online Review Systems." Proceedings of *ACM Conference on Computer and Communications Security* (**CCS**), Dallas, TX, October 2017.

[6] Yanzi Zhu, **Yuanshun Yao**, Ben Y. Zhao and Haitao Zheng. "Object Recognition and Navigation using a Single Networking Device." Proceedings of *International Conference on Mobile Systems, Applications, and Services* (**MobiSys**), Niagara Falls, NY, June 2017.

[7] Zhijing Li, Ana Nika, Xinyi Zhang, Yanzi Zhu, **Yuanshun Yao**, Ben Y. Zhao and Haitao Zheng. "Identifying Value in Crowdsourced Wireless Signal Measurements." Proceedings of *World Wide Web Conference* (**WWW**), Perth, Australia, April 2017.

[8] Zhijing Li, Ana Nika, Xinyi Zhang, Yanzi Zhu, **Yuanshun Yao**, Ben Y. Zhao and Haitao Zheng. "Identifying Value in Crowdsourced Wireless Signal Measurements." Workshop Poster on *Mobile Computing Systems and Applications* (**HotMobile**), Sonoma, CA, February 2017.

[9] Xi C. Chen, **Yuanshun Yao**, Sichao Shi, Snigdhansu Chatterjee, Vipin Kumar and James H. Faghmous. "A General Framework to Increase the Robustness of Model-based Change Point Detection Algorithms to Outliers and Noise." Proceedings of *SIAM International Conference on Data Mining* (**SDM**), Miami, FL, May 2016.

[10] James H. Faghmous, Ivy Frenger, **Yuanshun Yao**, Robert Warmka, Aron Lindel and Vipin Kumar. "A Daily Global Mesoscale Ocean Eddy Dataset From Satellite Altimetry." *Scientific Data 2, Nature Publishing Group*, June 2015.

Industry Experience

06/2018-09/2018 **Google** Sunnyvale, CA

Software Engineering Intern at Security & Privacy (Safe Browsing)

- Trained machine learning models to detect mobile malware on a global scale
- Improved model interpretability for malware manual analysts
- Diagnosed feature engineering and model training, implemented the improved training pipeline
- Investigated and analyzed feasibility of deep neural network models

06/2017-09/2017 **Google** Mountain View, CA

Software Engineering Intern at Google Shopping

- Trained deep neural network models (Faster R-CNN, SSD, R-FCN and Mask R-CNN) to recognize and localize commodities in shopping images
- Improved model performance with online hard example mining
- Implemented and demonstrated a prototype of sketch-based image retrieval system using deep learning models

06/2013-05/2014 **IBM** Princeton, NJ

Software Engineering Intern

- Worked on agile software development of IBM InfoSphere Optim Test Data Management
- Implemented data model generation using Eclipse Modeling Framework, interacting with various databases (Oracle, IBM DB2, SQL Server, Informix, Sybase, Netezza etc.)
- Implemented a prototype of machine learning system that predicts customer behaviors from transaction data

Research Experience

09/2017-present Graduate Student Researcher, Department of Computer Science, University of Chicago

- Advisor: Prof. Ben Y. Zhao and Prof. Heather Zheng
- Machine Learning, Deep Learning, Security and Privacy, Mobile Computing

01/2016-06/2017 Graduate Student Researcher, Department of Computer Science, UCSB

- Advisor: Prof. Ben Y. Zhao and Prof. Heather Zheng

07/2015-12/2015 Undergraduate Research Assistant, Department of Comp Sci and Eng, UMN

- Advisor: Prof. Vipin Kumar
- Spatio-temporal data mining research

Awards

2018 UU Fellowship, University of Chicago
2011-2015 Dean's list, University of Minnesota
2011-2015 Maroon Global Excellence Scholarship, University of Minnesota
2014 Undergraduate Research Opportunity Program Grant, University of Minnesota
2014 NSF Student Travel Grant

Teaching Experience

Spring 2016 CS 16 Problem Solving with Computers I, University of California, Santa Barbara
Winter 2016 CS 16 Problem Solving with Computers I, University of California, Santa Barbara
Fall 2015 CS 8 Introduction to Computer Science, University of California, Santa Barbara
Spring 2015 Csci 2033 Elementary Computational Linear Algebra, University of Minnesota
Spring 2013 Math 5651 Basic Theory of Probability and Statistics, University of Minnesota

In the Press

12/16/2017	Artificial intelligence is killing the uncanny valley and our grasp on reality. **Wired**. https://www.wired.com/story/future-of-artificial-intelligence-2018.
10/16/2017	Could AI be the future of fake news and product reviews?. **Scientific American**. https://www.scientificamerican.com/article/could-ai-be-the-future-of-fake-news-and-product-reviews.
09/05/2017	Many people can't tell the difference between Yelp reviews written by an AI and a human. Can you?. **Forbes**. https://www.forbes.com/sites/kevinmurnane/2017/09/05/many-people-cant-tell-the-difference-between-yelp-reviews-written-by-an-ai-and-a-human-can-you.
09/01/2017	AI writes Yelp reviews that pass for the real thing. **Engadget**. https://www.engadget.com/2017/09/01/ai-fake-yelp-reviews.
08/31/2017	AI trained on Yelp data writes fake restaurant reviews 'indistinguishable' from real deal. **The Verge**. https://www.theverge.com/2017/8/31/16232180/ai-fake-reviews-yelp-amazon.
08/31/2017	Robots learned how to write fake Yelp reviews like a human. **New York Post**. https://nypost.com/2017/08/31/robots-learned-how-to-write-fake-yelp-reviews-like-a-human.
08/30/2017	AI writes believable fake Yelp reviews. **Nvidia Developer**. https://news.developer.nvidia.com/ai-writes-believable-fake-yelp-reviews.
08/30/2017	Restaurant reviews could be generated by AI without you noticing. **Fortune**. https://fortune.com/2017/08/30/researchers-teach-ai-to-write-fake-reviews.
08/29/2017	Researchers taught AI to write totally believable fake reviews, and the implications are terrifying. **Business Insider**. https://www.businessinsider.com/researchers-teach-ai-neural-network-write-fake-reviews-fake-news-2017-8.