

# Tong Wu

9015 Eager Road #194, Richmond Heights, MO 63144  
tongwu98@outlook.com | 765-720-4989 | <https://tongwu2020.github.io/tongwu/>

## EDUCATION

### Washington University in St. Louis – GPA: 4.0/4.0

St. Louis, MO

Bachelor/Master of Science; Computer Science Major; Mathematics Major;

Sep 2018 - May 2021

**Honors:** Graduate Affiliation Scholarship, Undergraduate Research Conference Travel Award

**Relevant Coursework:** Adversarial Artificial Intelligence (A, graduate), Computer Vision (A, graduate), Bayesian Machine Learning (A, graduate), Applications of Deep Neural Networks (A+, graduate), Analysis of Imaging Data (A, graduate)

### DePauw University, College of Liberal Arts – GPA: 3.94/4.0 (Major GPA: 4.0/4.0)

Greencastle, IN

Bachelor of Arts; Pre-Engineering Major; Mathematics Minor;

Sep 2016 - May 2018

**Honors:** Dean's List for all semesters, DePauw Merit Scholarship

**Relevant Coursework:** Statistical Computing (A), Data Structures (A), Object-Oriented Software Development (A)

## PUBLICATION

- **Tong Wu**, Liang Tong and Yevgeniy Vorobeychik. "Defending Against Physically Realizable Attacks on Image Classification". In Proceedings of the 8th International Conference on Learning Representations (ICLR), May 2020. (Spotlight, acceptance rate 6.01%)
- Shaojie Wang, **Tong Wu**, Yevgeniy Vorobeychik, "Towards Robust Sensor Fusion in Visual Perception" (Preprint)

## EXPERIENCE

### Defending against Physically Realizable Attacks on Image Classification (ICLR 2020, Spotlight)

St. Louis, MO

Research Intern supervised by Prof. Yevgeniy Vorobeychik

Dec 2018 - Sep 2019

- Studied the problem of defending deep neural network approaches for image classification from physically realizable attacks
- Demonstrated that the state-of-the-art robust models exhibit limited effectiveness against three highest profile physical attacks
- Proposed a new abstract model, ROA, in which an adversary placed a small crafted rectangle that fooled the image classifier
- Adversarial Training using our ROA achieved much better robustness against physically realizable attacks than all SOTA models

### Robustness of Speaker Recognition and Identification

Remote caused by COVID19

Research Intern in *Cleverhans Lab*

May 2020 - Present

- Implemented the state-of-the-art speaker recognition and identification system via Tensorflow 2.0, achieved comparable results with benchmark results for more than 100 GB dataset with more than 1000 identities
- Analyzed the robustness of the whole pipeline including dither, Preemphasis, short time Fourier transform and convolutional neural network, developed a new attack through griffin-lim reconstruction to fool the speaker recognition system

### Towards Robust Sensor Fusion in Visual Perception

St. Louis, MO

Research Intern in *TRustworthy Autonomous Systems Engineering Lab*

Dec 2019 - May 2020

- Evaluated the robustness of RGB image classification and LiDAR sensor fusion for binary classification and object detection
- Posted attacks on both sensors, presented LiDAR could boost a huge amount of robustness compared to image classification against adversarial examples in autonomous driving settings

### Washington University in St. Louis

St. Louis, MO

Teaching Assistant of *Introduction to Machine Learning*

Jan 2019 - Present

- Collaborated with Professor to lead all teaching assistants on determining and evaluating the rubrics for assignments
- Hold regular office hour every week, helped students on course materials especially theoretical analysis of machine learning
- Advised and helped students build machine learning algorithms including Logistic Regression, Bagging and AdaBoost
- Graded students' lab assignments and exams; primarily checking the mathematical proof and coding efficiency and functionality

## SKILLS, HONORS & INTERESTS

**Programming Languages:** (Proficient)Python, (Proficient)R, (Proficient)MATLAB, C++, experienced with Java, Mathematica

**DL Framework & Other Techniques:** Pytorch, TensorFlow, Keras, Scikit-Learn, Numpy, Pandas, OpenCV and Linux

**Other Honors:** Michigan Competition MATH Challenge 3/74, Putnam Mathematical Competition top 10%

**Activities:** Review of AAAI 2021, Volunteer of ICLR 2020 & ICML 2020, Member of Tau Beta Pi Association, DePauw Science Research Fellow and Go Game Player