Jinghan Yang

Ph.D. in Computer Science and Engineering

☎ *+1 (617) 992 4573*
✉ *jinghan.yang@wustl.edu*
jinghany.github.io/website
in *Jinghan Yang*
jinghanY

Education

2017–present **Ph.D. in Computer Science and Engineering** Washington University in St. Louis *(St. Louis, USA) GPA 3.91.*
Thesis: Physically Realizable Attacks and Defenses for Autonomous Driving Systems.
Advisor: Yevgeniy Vorobeychik

2014-2016 **M.S in Applied and Financial Mathematics** Northeastern University *(Boston, USA) GPA 3.84.*
Advisors: Javed A. Aslam and Virgil Pavlu.

2010–2014 **B.S in Financial Mathematics** Tianjin University of Finance and Economics *(Tianjin, China) GPA 3.92.*
Advisors: Wei Geng and Shuhua Zhang.

Interests

My research interests fall broadly within the fields of adversarial machine learning, deep learning, and reinforcement learning. Throughout my Ph.D. I have explored the vulnerabilities of deep learning models in the context of computer vision as well as autonomous driving. I am particularly interested in the development of deep learning models for autonomous driving, and my recent work has focused on designing self-diving systems which are robust to both adversarial perturbations (e.g., malicious graffiti painted on road signs) as well as natural changes in the driving environment (e.g., weather, construction, or accidents). Recently I have also been working on robust algorithms for multi-agent deep reinforcement learning.

Research Experience

2017-present Ph.D. Research: My research has focused on the vulnerability of deep learning models. In particular, I have focused on developing attacks and defenses in the contexts of computer vision and autonomous driving. My thesis work aims to provide models for self-driving systems in the presence of natural and adversarial noise.
advisor: Yevgeniy Vorobeychik

2016-2017 Masters Research: This research project focused on developing a pipeline for efficient learning in the context of natural language classification. We developed an algorithm for hyperparameter selection of gradient-boosting methods. In particular, we found that this algorithm was effective at speeding-up training via the selection of regularization hyperparameters.
advisors: Javed A. Aslam and Virgil Pavlu

2013-2014 Undergraduate Research: This project analyzed the impacts of international trading on fluctuations in market pricing. To perform this analysis, we collected large amounts of data on assets traded within China. We used regression techniques to model the joint relationships between these assists and then measured the change in the joint relationships when other countries began trading these assets .
advisor: Wei Geng

2012-2013 Undergraduate Research: This research project focused on capturing the correlations between elements of macroeconomics (e.g., GDP of countries) and measurements of climate change. We modeled these relationships via systems of differential equations and used MatLab as a solver when conducting experiments .
adivsor: Shuhua Zhang

Papers

Publications

[1] Location Spoofing Attacks on Autonomous Fleets.
Jinghan Yang, Andrew Estornell, Yevgeniy Vorobeychik (NDSS *VehicleSec* 2023)

[2] Certified Robust Control under Adversarial Perturbations, [To appear (IEEE-ACC 2023)] .
Jinghan Yang, Hunmin Kim, Wenbin Wan, Naira Hovakimyan, Yevgeniy Vorobeychik

[3] Finding Adversarial Examples for Simulated Autonomous Driving with Fast and Differentiable Image Compositing, (AAAI TRASE 2022).
Jinghan Yang, Adith Boloor, Ayan Chakrabarti, Xuan Zhang, Yevgeniy Vorobeychik

[4] PROVES: Establishing Image Provenance using Semantic Signatures, (WACV 2021).
Mingyang Xie, Manav Kulshrestha, Shaojie Wang, **Jinghan Yang**, Ayan Chakrabarti, Ning Zhang, Yevgeniy Vorobeychik

[5] Protecting Geolocation Privacy of Photo Collections, (AAAI 2020).
Jinghan Yang, Ayan Chakrabarti, Yevgeniy Vorobeychik

Under Review

[6] Defending Patch Attacks via Semantic Analysis; 2023.
Jinghan Yang, Andrew Estornell, Adith Boloor, Yevgeniy Vorobeychik

Contributed Talks

2023 [To present] Oral Presentation for “Certified Robust Control under Adversarial Perturbation" at IEEE-ACC 2023.

2022 Oral Presentation for “A Fast and Differentiable Adversarial Testing Framework for Simulated Autonomous Driving" at AAAI 2022.

2020 Oral Presentation for “Protecting Geolocation Privacy of Photo Collections" at AAAI 2020.

2019 Oral Presentation for our developed autonomous driving vehicle in "CARLA Autonomous Driving Challenge" at CVPR 2019.

Programing and Software

Open-Source Software Projects

2023 **Certified Robust Control under Adversarial Perturbations** This software provides a self-driving agent (comprised of both a perception and control module) which is certifiably robust to adversarial noise. This agent can be deployed in any vision-based autonomous driving simulator and physical world. This software accompanies our IEEE-ACC paper of the same name .
`https://github.com/jinghanY/RobustControl`

2021 **Finding Adversarial Examples for Simulated Autonomous Driving with Fast and Differentiable Image Compositing** This software provides a differentiable proxy for the CARLA autonomous driving simulator. This allows researchers to more efficiently study attacks and defenses for simulated autonomous driving by subverting the computational issues which arise from the non-differentiability of simulators. This software accompanies our AAAI TRASE paper of the same name .
`https://github.com/jinghanY/physicalAttackImageComposition`

2020 **PROVES: Establishing Image Provenance using Semantic Signature** This software provides users with a learning framework which can certify facial images in order to prevent their use in constructing deep-fakes This software accompanies our WACV paper of the same name .
`https://github.com/jinghanY/imgprov`

2020 **Protecting Geolocation Privacy of Photo Collection** This software allows users to protect the geolocation of their publicly shared photo collections. Using deep learning models we modify the photo collection such the geolocation is no longer identifiable. This software accompanies our AAAI paper of the same name .
`https://github.com/jinghanY/geoPrivacyAlbum`

2019 **Autonomous Driving Agent for the CARAL Simulator** This software provides a self-driving agent for use in the CARAL simulator (achieved third-place in CVPR CARLA Autonomous Driving Challenge 2019).
`https://github.com/jinghanY/AutonomousDrivingAgent`

Programming Languages/Libraries

Fluent: Python, Tensorflow, Pytorch

Experienced: Java, C++, Matlab, R

Honors and Awards

2019 Third-place in the CARLA Autonomous Driving Challenge.

2013 Tianjin University in Finance and Economics Scholarship for the Rank-1 student.

2013 National Scholarship for Outstanding Undergraduates.

2012 Tianjin University in Finance and Economics Scholarship for the Rank-1 student.

2012 First Place in China's National Undergraduate Mathematical Modeling Contest.

Internships

Jan.-Apr. 2014 **Quantitative Analyst Intern**.
Sun and Bright Asset Management Company, Beijing, China

I was responsible for developing statistical tools which analyzed the financial reports of companies on the Chinese stock exchange in order to determine in Sub and Bright should invest-in, or acquire, those companies. Additionally, I helped develop efficient software methods for options pricing via a modified Black-Scholes Equation.

July 2012 **Data Analyst Intern**.
MassMutual Financial Group, Hong Kong, China

I was responsible for developing statistical tools which were used to analyze user questionnaires regarding insurance coverage and pricing.

Academic Development

Teaching

2021 Teaching Assistant for *AI for Social Impact Course*. (Washington Univerisity in St. Louis)

Peer Reviews

AAAI (2022, 2021, 2020), NeurIPS (2022, 2021), KDD (2021), AAMAS (2022, 2021), ICDM (2019)