

Huichen Li

✉ huichenli.cs@gmail.com

Education

Aug. 2018 - May. 2023 (expected): Ph.D. candidate *Computer Science*.

Department of Computer Science, University of Illinois Urbana-Champaign, US

○ GPA: 4.0/4.0

2014 - 2018: Bachelor of Engineering *Computer Science and Technology*.

ACM Honors Class, Zhiyuan College, Shanghai Jiao Tong University, China

○ GPA: 3.78/4.3;

Publications

Exploring Adversarial Robustness of Multi-Sensor Perception Systems in Self Driving,

James Tu, [Huichen Li](#), Xinchun Yan, Mengye Ren, Yun Chen, Ming Liang, Eilyan Bitar, Ersin Yumer, Raquel Urtasun.

○ Appeared at CoRL2021 (arXiv link).

Progressive-Scale Boundary Blackbox Attack via Projective Gradient Estimation,

Jiawei Zhang*, Linyi Li*, [Huichen Li](#), Xiaolu Zhang, Shuang Yang, Bo Li.

○ Appeared at ICML2021 (arXiv link).

Nonlinear Projection Based Gradient Estimation for Query Efficient Blackbox Attacks,

[Huichen Li](#)*, Linyi Li*, Xiaojun Xu, Xiaolu Zhang, Shuang Yang, Bo Li.

○ Appeared at AISTATS2021 (paper link).

Detecting AI Trojans Using Meta Neural Analysis,

Xiaojun Xu, Qi Wang, [Huichen Li](#), Nikita Borisov, Carl A. Gunter, Bo Li.

○ Appeared at IEEE Symposium on Security and Privacy 2021 (paper link).

QEBA: Query-Efficient Boundary-Based Blackbox Attack,

[Huichen Li](#)*, Xiaojun Xu*, Xiaolu Zhang, Shuang Yang, Bo Li.

○ Appeared at CVPR2020 (paper link);

A Machine Learning Approach To Prevent Malicious Calls Over Telephony Networks,

[Huichen Li](#), Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, Dawn Song.

○ Appeared at IEEE Symposium on Security and Privacy 2018 (paper link);

○ My conference talk (YouTube link).

The symbol * indicates equal contribution.

Preprints and Submissions

Learning to Watermark with Meta-Learning, [Huichen Li](#), Xiaojun Xu, Yu Cheng, Bo Li.

○ In submission.

Exploring the Limit of 3D Object Detection through UnAdversarial Examples, [Huichen Li](#), Chenxi Liu, Mahyar Najibi, Charles R. Qi, Yin Zhou, Mingxing Tan.

○ In submission.

On the Adversarial Robustness of Visual Question Answering Models, [Huichen Li](#), Boxin Wang, Ao Sun, Linjie Li, Zhe Gan, Bo Li.

- In submission.

BIFS: Backdoored Instance Detection and Mitigation via Feature Sensitivity Measurements,
Huichen Li, Xiaojun Xu, Bo Li.

- In submission.

Compromised ACC vehicles can degrade current mixed-autonomy traffic performance while remaining stealthy against detection,

George Gunter, Huichen Li, Avesta Hojjati, Matthew Nice, Matthew Bunting, Carl A. Gunter, Bo Li, Jonathan Sprinkle, Daniel Work.

- In submission. Preprint (arXiv link)

Data Poisoning Attack against Unsupervised Node Embedding Methods,

Mingjie Sun, Jian Tang, Huichen Li, Bo Li, Chaowei Xiao, Yao Chen, Dawn Song.

- Preprint (arXiv link).

Internships

May. 2022 - Nov. 2022: Waymo *Exploring UnAdversarial Examples for 3D Object Detection*, Research Intern.

Jun. 2020 - Aug. 2020: Uber ATG *Multi-modality Adversarial Robustness*, Research Intern.

Jun. 2019 - Aug. 2019: Ant Financial *Adversarial Attack on Image Recognition*, Research Intern.

Jun. 2018 - Jul. 2018: Tencent Technology *Adversarial Attack on Graph*, Research Intern.

Experience

Aug. 2018 - May. 2020: Research Assistant *Adversarial Machine Learning*, Prof. Bo Li, University of Illinois Urbana-Champaign, US.

Jun. 2017 - Dec. 2017: Research Intern *Low Rank Optimization*, Prof. Madeleine Udell & Prof. Nathan Kallus, Cornell University, US.

Sep. 2017 - Nov. 2017: Research Intern (Remote) *Large-scale Phone Call Network Analysis and Malicious Call Prevention*, Prof. Dawn Song, University of California, Berkeley, US.

Sep. 2016 - May. 2017: Research Intern *Early Spam Detection in Phone Call Network*, Prof. Yong Yu & Prof. Weinan Zhang, Shanghai Jiao Tong University, China.

Honors

Chirag Foundation Graduate Fellowship in Computer Science *The Department of Computer Science*, University of Illinois Urbana-Champaign, US.

Outstanding Graduates, Shanghai Jiao Tong University, China.

Kaiyuan Scholarship, Shanghai Jiao Tong University, China.

Scholarship of SJTU, Shanghai Jiao Tong University, China.

Zhiyuan Honored Scholarship *Zhiyuan College*, Shanghai Jiao Tong University, China.

Awards

1st Prize *Deep Learning and Security Innovation Hackathon @ Singapore, 2017.*

Champion *China Collegiate Programming Contest Female Final (CCPC-FF) 2016.*

Honorable Mention *2017 Mathematical Contest In Modeling.*

Academic Services

Conference Paper Reviewer / Program Committee Member: NeurIPS 2020/2021; ICLR2022; CVPR 2021/2022/2023; ICCV 2021; AAAI 2020/2021; AISTATS 2021; SSMLS (workshop) 2021; AdvML (workshop) 2020/2021; SPML (workshop) 2019; ICML Workshop on Socially Responsible Machine Learning 2021.

Journal Reviewer: Transactions on Computer-Aided Design of Integrated Circuits and Systems;

Teaching Assistant: Machine Learning, UIUC, 2022/2023; Advanced Topics in Security, Privacy and Machine Learning, UIUC, 2021; Advanced Computer Security, UIUC, 2020; Compiler Principle, SJTU, 2017.

Student Mentor: ALERT Program, UIUC

Language and Arts

English:

- TOEFL iBT: Total 109/120, Reading 26/30, Listening 29/30, Speaking 27/30, Writing 27/30
- GRE General Test: Verbal 159/170, Quantitative 170/170, Analytical Writing 4/6

Erhu: A traditional Chinese bowed string instrument. Professional Level A with certificate from Zhejiang Province Musicians Association in China.

Latest update date: March 22, 2023