

BINGYIN ZHAO

(+1)585-748-1626 bingyiz@g.clemson.edu

EDUCATION

CLEMSON UNIVERSITY Jan. 2018 – May. 2024
Ph.D. in ELECTRICAL AND COMPUTER ENGINEERING GPA: 4.0

ROCHESTER INSTITUTE OF TECHNOLOGY Aug. 2012 – Sep. 2014
Master of Science in ELECTRICAL ENGINEERING

EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY Aug. 2008 – Jun. 2012
Bachelor of Science in ELECTRICAL ENGINEERING

SKILLS

Knowledge Deep learning, Computer Vision, Adversarial/Robust machine learning, Model compression
Language & Tool Python, Pytorch, TensorFlow/Keras, Numpy, Scikit-learn, Pandas, Vim, Docker, Git, Shell, \LaTeX

WORKING EXPERIENCE

Deep Learning Software and Research Intern (AV Perception) May. 2022 – Feb. 2023
NVIDIA, Santa Clara, CA, Under supervision of Dr. Jose Alvarez and Dr. Zhiding Yu

- Conduct research on zero-shot robustness of ViT-based neural networks against natural corruptions such as weather conditions and natural adversarial examples.

Project Engineer Sep. 2015 – Nov. 2017
HYC USA Inc., San Jose, CA

- Worked on the design of touch/sensing test solutions for iPhone and Google Pixel.
- Coordinated design, quality, manufacturing, and operation teams to resolve production issues.

ASIC Design Engineer Intern Nov. 2014 – Mar. 2015
OmniVision Technologies, Inc., Santa Clara, CA

- Developed automated flow (scripted in Python, Perl, and Tcl) of chip power estimation, data analysis, and module-based power consumption analysis and integrated it into Cadence RC tools.

RESEARCH AND PROJECTS

Design of Robust Vision Transformers (*Pytorch/TensorFlow/Python*) May. 2022 – Mar. 2023

- Proposed a novel training paradigm that jointly incorporates self-emerging token labels and image-level labels and significantly enhanced clean accuracy and zero-shot robustness of Fully Attentional Networks on image classification and segmentation tasks.
- Achieved SOTA zero-shot robustness on ImageNet-A, ImageNet-R and Cityscape-C with model size of 77.3M.
- Experience with distributed training and parameter tuning of neural networks on GPU clustering such as NGC and Maglev.

Robust DNNs against Poisoning Attacks (*Pytorch/TensorFlow/Python*) Sep. 2018 – May. 2022

- Devised a general and scalable defensive framework against clean-label backdoor attacks towards image classification tasks. Achieved up to 100% detection rate and reduced attack success rate from $\sim 90\%$ to 0% against three widespread attacks.
- Proposed a novel defense against poisoning attacks using gradual magnitude pruning. Analyzed the correlation between pruning and model robustness and improved the post-attack accuracy from 5% to over 50%.

Clean-Label Poisoning Attacks towards DNNs (*Keras/Pytorch/Python*) Jun. 2020 – May. 2021

- Designed a generative adversarial net (GAN)-based framework for clean-label poisoned data generation that degrades the overall model accuracy.
- Built the framework using BigGAN architecture and devised a triplet loss function to improve the effectiveness and fidelity of poisoned data.
- Achieved 18% accuracy drop with only 20% poisoning ratio and 55% accuracy drop with full poisoning on modern neural networks such as ResNet, VGG and Inception-V3.

Class-Oriented Poisoning Attacks (*Keras/TensorFlow/Python*) Jun. 2019 – Jun. 2020

- Proposed an innovative poisoning attack that manipulates the predictions of neural networks on a per-class basis.
- Designed gradient-based and class-oriented algorithms to efficiently generate poisoned data at a large scale.

PUBLICATIONS

B. Zhao, Z. Yu, S. Lan, Y. Cheng, A. Anandkumar, Y. Lao and J. Alvarez, Fully Attentional Networks with Self-emerging Token Labeling

2023 IEEE/CVF International Conference on Computer Vision (ICCV)

B. Zhao, L. Qiu and Y. Lao, Data-Driven Feature Selection Framework for Approximate Circuit Design

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

A. Wang, B. Zhao and Y. Lao, Neural Network Fault Attacks Detection Using Gradient-Based Test Vector Generation

60th ACM/IEEE Design Automation Conference (DAC-23)

B. Zhao and Y. Lao, CLPA: Clean-Label Poisoning Availability Attacks Using Generative Adversarial Nets

Thirty-Sixth AAAI Conference on Artificial Intelligence (AAAI-22)

B. Zhao and Y. Lao, Towards Class-Oriented Poisoning Attacks Against Neural Networks

2022 IEEE Winter Conference on Applications of Computer Vision (WACV)

B. Zhao and Y. Lao, Resilience of Pruned Neural Network Against Poisoning Attack

2018 13th International Conference on Malicious and Unwanted Software (MALWARE)

B. Zhao and Y. Lao, UltraClean: A Simple Framework to Train Robust Neural Networks against Backdoor Attacks

Thirty-Eighth AAAI Conference on Artificial Intelligence

(Under Review)