Yaning Jia

jiayaning@hust.edu.cn
(+86) 13081860420
Huazhong University with Science and Technology (HUST), Wuhan, China

Homepage:
https://github.com/YaningJia

EDUCATION

Master student, Cyberspace Security Sep. 2021 - Present
Huazhong University with Science and Technology, Wuhan, China
School of Cyberspace Security
Work with Prof. Hongfei Wang

B.S., Computer Science Sep. 2017 - Jun. 2021
Northeastern University, China
School of Computer and Communication Engineering
GPA: 4.00

EXPERIENCE

Research Assistant Jun. 2022-Mar. 2023
Duke University and Duke Kunshan University, US, China
School of Data Science
Mentors: Prof. Dongmian Zou

Researched Lipschitz property and proposed a general frameworks for deep neural networks from a perspective of Lipschitz, which improves stability of network models and enhance their robustness against adversarial attacks and noisy data. Also, the algorithm can serve as a plug-in component, enhancing the overall robustness of models.

Research Assistant Mar. 2023-Jun. 2023
Brandeis University, Waltham, Massachusetts, US
Michtom School of Computer Science
Work with Chunhui Zhang, Prof. Chunxu Zhang, Prof. Jundong Li

Developed a novel fairness method for deep neural networks that focuses on ensuring individual fairness. Compared previous methods, this method, integrated into network models, significantly enhances individual fairness with lower time cost while retains performance.

Research Assistant Jun. 2023-Present
Zhejiang Lab, National Lab at China, Hangzhou
Institute of Artificial Intelligence

I am currently engaged in research on large-scale graph pre-training models, focusing on large transformer model acceleration , and exploring the feasibility of Transformer model acceleration from a theoretical perspective.

RESEARCH INTEREST

- Stability of Deep Learning*(e.g., my KDD'23 on Adversarial attacks of DNNs)*
- Machine Learning Fairness *(e.g., my ICLM'23 workshop on individual fairness of DNNs)*

PAPER

- **Yaning Jia**, Dongmian Zou, Hongfei Wang, Hjin. Enhancing Node-Level Adversarial Defenses by Lipschitz Regularization of Graph Neural Networks, *the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**), 2023*.
- **Yaning Jia**, Chunhui Zhang. Stabilizing GNN for Fairness via Lipschitz Bounds, *New Frontiers in Adversarial Machine Learning **(AdvML@ICML)**, 2023.*
- **Yaning Jia**, Chunhui Zhang, Jundong Li, Chuxu Zhang. Characterizing Lipschitz Stability of GNN for Fairness, *on submission & extension of my AdvML@ICML'23 paper.*

SKILLS

Programming Skills: C++, Python, java, PyTorch, MATLAB, Git, PyG, DGL
Operating System: Linux

ACTIVITIES

- Conference official reviewer for ICML2023 workshop, KDD2023 workshop

Latest Update: June 2023