Xiangchi Yuan

781-290-7437 | xiangchiyuan@brandeis.edu | Website | github

Education

Brandeis University — Waltham, MA, USA
M.S.in Computer Science — *Aug. 2022 – May 2024*

University of Electronic Science and Technology of China (UESTC) — Chengdu, Sichuan, CN
B.Eng. in Electronic and Information Engineering — *Aug. 2018 – May 2022*

Research Interests

Graph Mining/Data Mining, Data-efficient AI, Trustworthy AI, Natural Language Processing.

Publications

[3] **Xiangchi Yuan**, Chunhui Zhang, Yijun Tian, and Chuxu Zhang. Exploring Anti-degraded Graph Robust Learning Against Adversarial Attacks. In Thirty-seventh Conference on Neural Information Processing Systems *(NeuIPS 2023 Under review)*.

[2] **Xiangchi Yuan**, Chunhui Zhang, Yijun Tian, and Chuxu Zhang. Navigating Graph Robust Learning against All-Intensity Attacks. In Fortieth International Conference on Machine Learning (ICML) 2023-New Frontiers in Adversarial Machine Learning Workshop *(ICML 2023 AdvML-Frontiers Workshop)*.

[1] Lang Qin, Yuntao Xie, Xinwen Liu, **Xiangchi Yuan**, and Huan Wang. An End-to-End 12-Leading Electrocardiogram Diagnosis System Based on Deformable Convolutional Neural Network With Good Antinoise Ability. In IEEE Transactions on Instrumentation and Measurement *(IEEE TIM 2021)* .

Research Experience

Research Assistant — Jul. 2023 – Present
The Pennsylvania State University — *University Park, PA, USA*
- Applied contrastive learning and data augmentation to Fine-tuning Bart for multi-attributes summarization.
- Designed Automatic Prompt Engineer for conditional context summarization by LLMs.

Research Assistant — Sep. 2022 – Jun. 2023
Brandeis University — *Waltham, MA, USA*
- Proposed Denoise Masked Graph Auto-encoder to remove malicious edges of the attacked graph.
- Revealed the connection between differential privacy(DP) and GNN robustness, and applied the idea of differential privacy to GNN to improve the robustness.
- Introduced the mixture-of-experts model to GNN layer to select the better DP experts against attacks.
- Provided a theoretical robust guarantee for designed Differential Privacy Mixture-of-Experts module.

Undergraduate Research Assistant — Sep. 2020 – Feb. 2021
University of Electronic Science and Technology of China — *Chengdu, Sichuan, CN*
- Designed Deformable Convolutional Neural Network With Good Antinoise Ability for ECG classification
- Classified different ECG signals for diagnosis with employing Tri-net combined Tri-training

Work Experience

Software Development Engineer Intern — Apr. 2022 – Jul. 2022
VeriSilicon Microelectronics, GPU Arch Group — *Chengdu, Sichuan, CN*
- Designed HDR adaptive curve fitting algorithm: meeting hardware requirements and keeping high precision.
- Implemented CCM gamut mapping which suits hardware with fixed-point calculation for different Gamut settings.
- This SoC IP was used in **Google Pixel**.

Honors

UESTC University-wide Outstanding Student Scholarship — Nov. 2020, Nov. 2021

Service

The Web Conference (WWW) 2023 — *Sub-reviewer*
The International Conference on Machine Learning (ICML) 2023 — *Sub-reviewer*