(+86) 188-1131-0021
xiaoyuliang@buaa.edu.cn
xiaoyuu-liang.github.io

Xiaoyu Liang

Education

School of Cyber Science and Technology, Beihang University Beijing, China
B.E. in Information Security Sep. 2019 - Jun. 2023

- GPA: 3.82/4
- Relevant coursework: Mathematical Analysis for Engineering, Advanced Algebra, Probability and Statistics, Machine Learning

School of Cyber Science and Technology, Beihang University Beijing, China
M.E. in Cyberspace Security Sep. 2023 - Jun. 2026 *(expected)*

- Advisor: Dr. Haohua Du
- GPA: 3.83/4
- Research Focus: Trustworthy Machine Learning, Diffusion Models
- Relevant coursework: Matrix Theory, Theory and Technology of Trusted Computing, AI Safety

Department of Computer Science, University College London London, UK
Visiting Research Student Sep. 2025 - Feb. 2026 *(expected)*

- Advisor: Prof. Lorenzo Cavallaro
- Research Program: Graph-based Adversarial Machine Learning for Code Models

Publications

1. **X. Liang**, H. Du, W. Ma, Y. Tian, X. Xu, "CiDer: A Black-box Approach to Classify Node with Certified Robustness Guarantees," *IEEE INFOCOM 2025*.
2. **X. Liang**, H. Du, H. Lu, F. Shang, "GRACED: A Plug-and-Play Solution for Certifiable Graph Classification," *IEEE ICASSP 2025*.
3. W. Ma, Z. Liu, H. Du, **X. Liang**, "Sedative: Pacify the Online Social Networks under Hijacking-based Troll Attacks," *IEEE/ACM IWQoS 2025*, (Accepted).

Research Experience

Robustness Certificate for Black-box Graph Neural Networks via Diffusion Model
Graduate Research Jan. 2024 - Oct. 2024

- Designed a black-box approach for GNN to defend against any malicious attacker.
- Developed an efficient graph diffusion model for adversarial graph purification.
- Implemented diffusion model and tested on multiple datasets for classification tasks.

Customized Noise Schedule in Diffusion Models for RF-Data
Graduate Research Nov. 2024 - May. 2025

- Investigated semantic characteristics of multi-wavelength radio-frequency datasets.
- Developed tailored diffusion noise schedules for diverse spectral data.

Graph-based Adversarial Attack against Malware Detection Systems
Graduate Research (Ongoing Work) Jun. 2025 - Present

- Investigating graph methods to preserve structure and scemantics of software.
- Exploring diffusion-based policy for adversarial malware reinforcement learning.

Acdemic Acitivities

CISPA ELLIS Summer School 2025 - Trustworthy AI Saarbruecken, Germany
Short-term Program Aug. 2025

- Poster: GRACED: A Plug-and-Play Solution for Certifiable Graph Classification

Awards & Honors

- **First Prize** (top 5%), National Collage Student Information Security Contest — Aug. 2022
- **Outstanding Graduate Award**, Beihang University — Jun. 2023
- **Outstanding Postgraduate Student**, Beihang University — May. 2025
- **First Prize of Academic Scholarship**, Beihang University — Nov. 2024
- **Second Prize of Academic Scholarship**, Beihang University — Nov. 2020-2023

Skills

Languages: English (C1 | IELTS: 7.5), Mandarin (native).
Programming Languages: Python, C, Java, SQL.
Frameworks and Libraries: PyTorch, PyTorch Geometric, PyTorch Lightning, Matplotlib.

References

Dr. Haohua Du

- Title: Assistant Professor
- Affiliation: School of Cyber Science and Technology, Beihang University
- Email: [duhaohua@buaa.edu.cn]

Dr. Tong Bai

- Title: Associate Professor
- Affiliation: School of Cyber Science and Technology, Beihang University
- Email: [tongbai@buaa.edu.cn]