ZHIYU NI

Email: zhiyuni@usc.edu Tel: (+1)323-633-1447

EDUCATION

Incoming UC Berkeley EECS PhD *From 2024.7*

University of Southern California (USC) *Los Angeles, United States*
Ph.D. *Computer Engineering*, Advisor: Pierluigi Nuzzo *2022.8 - Present*

Research Interest:
Trustworthy Machine Learning (Security, Privacy), Anomaly Detection

University of Science and Technology of China (USTC) *Hefei, China*
B.S. *Physics*, Outstanding Graduates *2018.8 - 2022.6*

PUBLICATIONS

Sparse but Strong: Crafting Adversarially Robust Graph Lottery Tickets
Subhajit Dutta Chowdhury*, **Zhiyu Ni***, Qingyuan Peng, Souvik Kundu, Pierluigi Nuzzo
GLFrontiers Workshop, NeurIPS 2023

Analyzing Adversarial Vulnerabilities of Graph Lottery tickets
Subhajit Dutta Chowdhury*, **Zhiyu Ni***, Qingyuan Peng, Souvik Kundu, Pierluigi Nuzzo
IEEE ICASSP 2024

RESEARCH EXPERIENCE

Exploring robustness of Graph Lottery Tickets against adversarial attacks

- Systematically analyzed the robustness of graph lottery tickets (GLT) against adversarial attacks.
- Proposed a new loss function for training robust yet sparse GLTs against poisoning and evasion attacks.

Privacy Protector: Defending GNNs against Inference Attacks

- Explored existing model compression methods as a defense against Inference Attacks on GNN.
- Developing a new training procedure leveraging weights pruning and knowledge distillation.

LLM for Anomaly Detection

- Exploring the capabilities of LLMs (ChatGpt, Llama, etc.) in terms of anomaly detection and encoding graph information into natural language.
- Designing in-context learning flow to enable LLMs to identify fraud and numerically evaluate performance in various datasets (YelpChi, AmazonChi).

WORK EXPERIENCE

Iflytek *Hefei, China*
Machine Learning Engineer Intern, *AI Research Institute* *2022.2 - 2022.6*

- Independently carried out machine translation tasks utilizing seamless bidirectional translation among English, German, Italian, and Portuguese languages.
- Surpassed Google Translation by attaining a superior BLEU score.

SKILLS

Python, C, PyTorch, DGL, Pytorch geometric, Unix shell, LaTeX