ZIHAO ZHU

Address: 2001 Longxiang Road, Shenzhen, China
Email: zihaozhu@link.cuhk.edu.cn | zhu.zihao@outlook.com

EDUCATION

The Chinese University of Hong Kong, Shenzhen, China *2021.09 - Present*
School of Data Science
Ph.D. of Data Science
Advisor: Baoyuan Wu

University of Chinese Academy of Sciences, Beijing, China *2018.09 - 2021.06*
Institute of Information Engineering GPA: 3.63
Master of Science in Engineering
Advisor: Yue Hu, Chuan Zhou

China University of Mining and Technology, Jiangsu, China *2014.09 - 2018.06*
School of Computer Science and Technology GPA: 3.75
Bachelor of Engineering
Advisor: Guan Yuan

RESEARCH INTERESTS

AI security & privacy, Backdoor attack and defense, Multimodal machine learning

RESEARCH EXPERIENCE

Shenzhen Research Institute of Big Data Shenzhen, China
Research Assistant at Secure Computing Lab of Big Data *2020.06-2021.09*

- Backdoor samples selection.

Institute of Information Engineering Beijing, China
Research Assistant at NELIST Lab *2017.06-2018.09*

- Visualize large-scale graph data at different levels based on graph neural networks.
- This module was used in a national project.

PUBLICATIONS

Journal (1 PR, 1 Under Review)

1. Adversarial Machine Learning: A Unified Perspective of Adversarial Examples, Backdoor Learning and Weight Attack
   Baoyuan Wu, Li Liu, **Zihao Zhu**, Yanbo Fan, Siwei Lyu, Hongyuan Zha
   submitted to IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2022
2. Cross-Modal Knowledge Reasoning for Knowledge-based Visual Question Answering
   Jing Yu*, **Zihao Zhu***, Yujing Wang, Weifeng Zhang, Yue Hu, Jianlong Tan
   In Pattern Recognition (PR), 2020

Conference (2 IJCAI, 2 ICASSP, 3 Under Review)

1. Enhanced Few-Shot Class-Incremental Learning via Ensemble Models
   Mingli Zhu, **Zihao Zhu**, Baoyuan Wu
   Submitted to NeurIPS, 2022

2. Learning to Optimize Permutation Flow Shop Scheduling via Graph-based Imitation Learning
   Longkang Li, Siyuan Liang, **Zihao Zhu**, Xiaochun Cao, Chris Ding, Hongyuan Zha, Baoyuan Wu
   Submitted to NeurIPS, 2022

3. BackdoorBench: A Comprehensive Benchmark of Backdoor Learning
   Baoyuan Wu, Hongrui Chen, Mingda Zhang, **Zihao Zhu**, Shaokui Wei, Danni Yuan, Hongyuan Zha
   Submitted to NeurIPS, 2022

4. From Shallow to Deep: Compositional Reasoning over Graphs for Visual Question Answering
   Zihao Zhu
   In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2022

5. MCR-NET: A Multi-Step Co-Interactive Relation Network for Unanswerable Questions on Machine Reading Comprehension
   Wei Peng, Yue Hu, Luxi Xing, Yuqiang Xie, **Zihao Zhu**, Yajing Sun
   In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021

6. Mucko: Multi-Layer Cross-Modal Knowledge Reasoning for Fact-based Visual Question Answering
   Zihao Zhu, Jing Yu, Yujing Wang, Yajing Sun, Yue Hu, Qi Wu
   In Proceedings of the 29th International Conference on Joint Artificial Intelligence (IJCAI), 2020

7. DAM: Deliberation, Abandon and Memory Networks for Generating Detailed and Non-repetitive Responses
   Xiaoze Jiang, Jing Yu, Zengchang Qin, **Zihao Zhu**, Qi Wu
   In Proceedings of the 29th International Conference on Joint Artificial Intelligence (IJCAI), 2020

PATENTS

- Graph Visualization Method based on Graph Convolution Network
  Zihao Zhu, Chuan Zhou, YaNan Cao, Peng Zhang, Li Guo
  China, CN109753589A

SERVICE

Reviewer:
AAAI 2020

TEACHING

MFE5260 Data Sciences in Financial Engineering — 2022 Spring
Teaching Assistant

DDA6309 Probabilistic Graphical Models — 2021 Fall
Teaching Assistant

AWARDS

AIRS Talent of PhD Research Program	2021.09
University of Chinese Academy of Sciences Merit Student	2020.10
Outstanding Undergraduate Thesis Award	2018.06
The First Prize Scholarship of CUMT	2016.10
The First Prize Scholarship of CUMT	2015.10

SKILLS

Programming skills:
C++, Python, JAVA