Min Liu

191240030@smail.nju.edu.cn · damianliumin.github.io
No.163 Xianlin Avenue, Nanjing, Jiangsu Province, China (210023)

Education

Nanjing University Sept. 2019 – June. 2023
B.S. in Computer Science and Technology, Kuang Yaming Honors School *Jiangsu, China*

- **GPA:** 4.57/5.00 (91.4/100) **Ranking:** 1st/15

Publications

[1] **Min Liu**, Xiangyu Yue, Alberto Sangiovanni Vincentelli, "Backdoor Suppressor: Relabeling and Stamping Poisoned Data for Safe Learning", in submission to *CVPR-23*

[2] **Min Liu**, Yu Bao, Chengqi Zhao, Shujian Huang, "Selective Knowledge Distillation for Non-Autoregressive Neural Machine Translation", in submission to *AAAI-23*

Research Experience

U.C. Berkeley, Industrial Cyber-Physical Center Jun. 2022 – Nov. 2022
Research Intern, supervised by Prof. Alberto Sangiovanni-Vincentelli and Dr. Xiangyu Yue *(remote) CA, US*

- Proposed the idea of backdooring poisoned samples to defend against backdoor attack on visual systems, which helps achieve successful defense with minor performance drop on clean data.
- Stamped and relabeled a small set of isolated backdoor samples to inject a non-adversarial backdoor which is triggered by the adversarial backdoor pattern.
- Introduced an efficient data filtering technique at testing stage based on different mechanism of the stamp on clean and poisoned samples.
- Paper submitted to CVPR-23.

Nanjing University, NLP Group Nov. 2021 – Jun. 2022
Research Intern, supervised by Associate Prof. Shujian Huang and Dr. Yu Bao *Jiangsu, China*

- Proposed selective knowledge distillation which introduces an evaluator to select NAT-friendly targets that enjoy both high quality and low complexity.
- Introduced a simple yet effective progressive distillation method to boost NAT performance.
- Realized a flexible trade-off between the quality and complexity of training data for NAT models.
- Demonstrated that distilling only 5% of the raw translations with selection suffices to help an NAT outperform its counterpart trained on raw data by a large margin.
- Paper under review in phase 2 of AAAI-23.

UNC, Kenan-Flagler Business School May. 2021 – Aug. 2021
Research Assistant, supervised by Assistant Prof. Yuqian Xu *(remote) NC, US*

- Analyzed data using statistical tools and machine learning techniques in several econometric projects.
- Employed the DID method coupled with matching to estimate the impact of mobile payment adoption and expansion on consumer bank credit card transaction activities through both offline and online channels, relying on a unique data set provided by a leading bank in Asia.
- Utilized data from one leading on-demand delivery platform in Asia to understand the learning process of gig workers, whose experience improves the operational outcome by reducing delivery time.

Nanjing University, State Key Laboratory for Novel Software Technology Jan. 2021 – May. 2021
Research Assistant, supervised by Associate Prof. Yuan Yao *Jiangsu, China*

- Investigated trojan attack on neural networks and gave a presentation to graduate students in Softwiser Group.
- Mitigated the effects of trojan triggers by pre-processing inputs with class-specific patterns.
- Generated patterns that break the dominance of trojan triggers when applied to attacked images based on an encoder-decoder framework trained on pairs of images with the same label.

Industry Experience

ByteDance, AI Lab Mar. 2022 – Dec. 2022
Algorithm Intern *Shanghai, China*

- Proposed a cross-modal pre-training method to build robust linguistic and acoustic knowledge representation.
- Forced cross-modal glance by masking self-attention of the shared encoder to reduce modality gap.
- Achieved a substantial improvement on the downstream tasks: speech recognition and translation.

Selected Projects

Autonomous Vehicle Sep. 2021 – Dec. 2021

- Participated in the design of a tiny car navigating in the office environment based on SLAM and path planning. Mainly responsible for message-passing through ROS. (NJU innovation and practice courses)

NANOS Mar. 2021 – Jul. 2021

- Implemented a multiprocessor operating system with physical memory management, kernel multi-threading and virtual file system.

NJU Emulator Sep. 2020 – Dec. 2020

- Implemented an emulator for x86 instructions, a machine-independent abstraction layer, and a virtual machine on top of this layer where some software and games can be directly launched.

Selected Honors

Huawei Scholarship *(1% in Kuang Yaming Honors School)*	Nov. 2022
National Elite Program Scholarship *(first prize, top 5% among elite program students)*	Dec. 2021
Gang Zheng Overseas Study Scholarship *(0.6% in Nanjing University)*	Dec. 2021
Dalian Institute of Chemical Physics Scholarship *(5% in Kuang Yaming Honors School)*	Dec. 2021
Yongman Yang Scholarship *(1% in Kuang Yaming Honors School)*	Nov. 2021
National Elite Program Scholarship *(first prize, top 5% among elite program students)*	Dec. 2020
People's Scholarship *(first prize, 3% in Nanjing University)*	Nov. 2020

Technical Skills

Languages	Chinese (native), English (TOEFL: 110)
Programming	Python, C/C++, MATLAB, Assembly, Verilog, HTML/CSS
Framework & Packages	PyTorch, NumPy, Pandas, OpenCV
Toolkits	Fairseq, PyBullet, MuJoCo