
YUWEI SUN

ywsun@g.ecc.u-tokyo.ac.jp | +81-8081165839

7 Chome-3-1 Hongo, Bunkyo City, Tokyo 113-8654, Japan

EDUCATION

The University of Tokyo	Tokyo, Japan
<i>Ph.D.</i> , Information Science and Technology GPA: 4.0/4.0	04-2021 ~ 03-2024 (anticipated)
Minor: International Graduate Program of Innovation for Intelligent World	
Thesis Topic: Modular Neural Networks, Meta Learning, Multimodality	
Supervisors: Hideya Ochiai, Jun Sakuma	
<i>M.S.</i> , Information and Communication Engineering (Hons.) GPA: 3.84/4.0	04-2019 ~ 03-2021
Honors: Department Chair's Award	
Thesis: Network Intrusion Detection Based on Distributed Trustworthy Artificial Intelligence	
Research Focus: Decentralized Neural Networks, AI Security and Privacy	
<i>Post-Graduate Research Program</i> , Graduate School of Information Science and Technology	10-2018 ~ 03-2019
Research Focus: Decentralized Neural Networks	
North China Electric Power University	Beijing, China
<i>B.S.</i> , Computer Science and Technology (Hons.)	09-2014 ~ 08-2018
Thesis: Attacks on Deep Learning Systems Based on Generative Adversarial Networks	
Research Focus: Computer Vision	

EXCHANGE EXPERIENCES

Massachusetts Institute of Technology	Cambridge, MA, US
<i>Fellow of the Advanced Study Program</i> , Graduate School of Engineering	02-2020 ~ 05-2020
Courses: Distributed neural circuits, Underactuated robotics, Blockchain	
University of Pennsylvania	Philadelphia, PA, US
<i>Visiting Student</i>	08-2019 ~ 10-2019
Waseda University	Tokyo, Japan
<i>Visiting Student</i>	10-2016 ~ 08-2017

EMPLOYMENT

Japan Society for the Promotion of Science (JSPS)	Tokyo, Japan
<i>Doctoral Course Research Fellow</i>	04-2022 ~ Present
RIKEN Center for Advanced Intelligence Project (AIP)	Tokyo, Japan
<i>PhD Student Researcher</i> , AI Security and Privacy Team	04-2021 ~ Present
RIKEN AIP is for the Advanced Integrated Intelligence Platform Project of the Japan MEXT	
<i>- Perform research on the security and generality of federated learning and multimodal models</i>	
The University of Tokyo	Tokyo, Japan
<i>Research Assistant</i> , Graduate School of Information Science and Technology	06-2020 ~ Present
United Nations University	Tokyo, Japan
<i>Systems Engineer Intern</i>	06-2020 ~ 12-2020
The United Nations University is the academic and research arm of the United Nations	
<i>- Performed research on privacy-preserving deep learning for cybersecurity</i>	
<i>Consultant</i>	05-2021 ~ 06-2022
<i>- Researched multi-source domain adaptation in federated learning for vision and text data</i>	

RESEARCH GRANTS

Current
- Japan Society for the Promotion of Science, Grant-in-Aid for JSPS Fellows, JPY1700k, 2022-2024
Previous
- Japan Science and Technology Agency, SPRING GX program, JPY340k, 2021-2022

SELECTED PUBLICATIONS

Journals

- **Yuwei Sun**, Hideya Ochiai, and Jun Sakuma. Attacking Distance-aware Attack: A Semi-targeted Poisoning Attack on Federated Learning. *IEEE Transactions on Artificial Intelligence*. 2023 (submitted)
- **Yuwei Sun** and Hideya Ochiai. Homogeneous Learning: Self-Attention Decentralized Deep Learning. *IEEE Access*, Vol.10, pp.7695-7703. 2022.
- **Yuwei Sun**, Hideya Ochiai, and Hiroshi Esaki. Decentralized Deep Learning for Multi-Access Edge Computing: A Survey on Communication Efficiency and Trustworthiness. *IEEE Transactions on Artificial Intelligence*. 2022.
- **Yuwei Sun**, Hideya Ochiai, and Hiroshi Esaki. Adaptive Intrusion Detection in the Networking of Large-Scale LANs with Segmented Federated Learning. *IEEE Open Journal of the Communications Society*, Vol.2, pp.102-112. 2020.

Conferences

- **Yuwei Sun**. Meta Learning in Decentralized Neural Networks: Towards More General AI. *AAAI/SIGAI Doctoral Consortium*. 2023.
- **Yuwei Sun** and Hideya Ochiai. UniCon: Unidirectional Split Learning with Contrastive Loss for Visual Question Answering. *NeurIPS Workshop on Self-Supervised Learning*. 2022.
- **Yuwei Sun**, Ng Chong, and Hideya Ochiai. Feature Distribution Matching for Federated Domain Generalization. *Asian Conference on Machine Learning (ACML)*. 2022.
- **Yuwei Sun**, Hideya Ochiai, and Jun Sakuma. Semi-Targeted Model Poisoning Attack on Federated Learning via Backward Error Analysis. *IEEE International Joint Conference on Neural Networks (IJCNN)*. 2022.
- **Yuwei Sun**, Ng Chong, and Hideya Ochiai. Network Flows-Based Malware Detection Using a Combined Approach of Crawling and Deep Learning. *IEEE International Conference on Communications (ICC)*. 2021.
- **Yuwei Sun**, Hideya Ochiai, and Hiroshi Esaki. Blockchain-Based Federated Learning Against End-Point Adversarial Data Corruption. *IEEE International Conference on Machine Learning and Applications*. 2020.
- **Yuwei Sun**, Hideya Ochiai, and Hiroshi Esaki. Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs. *IEEE International Joint Conference on Neural Networks (IJCNN)*. 2020.

HONORS AND AWARDS

- Heiwa Nakajima Foundation Scholarship 2021
- The University of Tokyo, International Student Scholarship 2019
- North China Electric Power University, Excellent Student Scholarship 2016
- COMAP Mathematical Contest in Modeling, Successful Participant 2015

SKILLS

Programming: Python (Advanced), PyTorch (Advanced), Tensorflow (Advanced), OpenCV (Advanced), Linux commands (Intermediate), Git (Intermediate), Docker (Intermediate), SQL (Intermediate), HTML (Intermediate), JavaScript (Elementary), C++ (Elementary), Java (Elementary)

AI Research Computer: RAIDEN by Fujitsu in RIKEN Center for Advanced Intelligence Project (AIP Center)

Languages: Chinese (native), English (TOEFL IBT 101/120), Japanese (JLPT N1 169/180)

OTHER ACTIVITIES

Academic Services

- Reviewer: IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Artificial Intelligence, Neural Networks, Engineering Applications of Artificial Intelligence, IEEE TII, IEEE TITS, ACM Multimedia, AISTATS, ECML PKDD, FUZZ-IEEE, IJCNN, IEEE CEC, ACML, NeurIPS, CVPR
- Volunteer for NeurIPS 2021

Doctoral Consortiums

- AAAI 2023 Doctoral Consortium
- IEEE CIS Student and Early Career Mentoring Program at IEEE WCCI 2022