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
Ph.D., Information Science and Technology GPA: 4.0/4.0 04-2021 ~ 03-2024 (anticipated)
Minor: International Graduate Program of Innovation for Intelligent World
Thesis: Localized Learning and Generalization in Artificial Neural Networks with Properties of the Global Workspace
Supervisor: Hideya Ochiai

M.S., Information and Communication Engineering (Hons.) GPA: 3.84/4.0 04-2019 ~ 03-2021
Honor: Department Chair's Award
Thesis: Network Intrusion Detection Based on Distributed Trustworthy Artificial Intelligence
Research Focus: Decentralized Neural Networks, AI Security and Privacy

Post-Graduate Research Program, Graduate School of Information Science and Technology 10-2018 ~ 03-2019
Research Focus: Decentralized Neural Networks

North China Electric Power University Beijing, China
B.S., 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
Fellow of the Advanced Study Program, Graduate School of Engineering 02-2020 ~ 05-2020
Courses: Distributed neural circuits (Brain and Cognitive Sciences), Underactuated robotics, Blockchain

University of Pennsylvania Philadelphia, PA, US
Visiting Student 08-2019 ~ 10-2019

Waseda University Tokyo, Japan
Visiting Student 10-2016 ~ 08-2017

EMPLOYMENT

Araya Tokyo, Japan
Research Assistant, Moonshot Program 04-2023 ~ Present
Program goal: Liberation from biological limitations via physical, cognitive, and perceptual augmentation
- Research NeuroAI and neuroscience-inspired attention and memory mechanism in Transformer models

Japan Society for the Promotion of Science Tokyo, Japan
Doctoral Course Research Fellow (DC2) 04-2022 ~ Present

RIKEN Center for Advanced Intelligence Project Tokyo, Japan
PhD Student Researcher, AI Security and Privacy Team 04-2021 ~ Present
RIKEN AIP is for the Advanced Integrated Intelligence Platform Project of the Japan MEXT
- Perform research on the security of localized learning and multimodal models

The University of Tokyo Tokyo, Japan
Research Assistant, Graduate School of Information Science and Technology 06-2020 ~ 05-2023

United Nations University Tokyo, Japan
Consultant, Computing Centre 05-2021 ~ 06-2022
The United Nations University is the academic and research arm of the United Nations
- Researched multi-source domain adaptation and its application in vision and text data

Research Intern 06-2020 ~ 12-2020
- Performed research on privacy-preserving decentralized machine learning

RESEARCH GRANTS

Current
- Microsoft Research Asia Collaborative Research Program (D-CORE 2023), JPY1270k, 2023-2024
- 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.*
- **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, Vol.3, No.6, pp.963-972. 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**, Hideya Ochiai, Zhirong Wu, Stephen Lin, Ryota Kanai. Associative Transformer is a Sparse Representation Learner. *NeurIPS Workshop on Associative Memory and Hopfield Networks. 2023.*
- **Yuwei Sun**. Meta Learning in Decentralized Neural Networks: Towards More General AI. *AAAI 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**, 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

- WBAI Incentive Award, Whole Brain Architecture Initiative, 2023
- AAAI Student Scholarship, 2023
- Heiwa Nakajima Foundation Scholarship, 2021
- International Student Scholarship, The University of Tokyo, 2019
- Excellent Student Scholarship, North China Electric Power University, 2016
- Successful Participant, COMAP Mathematical Contest in Modeling, 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
Languages: Chinese (native), English (TOEFL IBT 101/120), Japanese (JLPT N1 169/180)

OTHER ACTIVITIES

Talks

- August 2023, "Localized Learning Through the Lens of Global Workspace Theory", a talk at the Consciousness Research Network (CoRN)
- April 2023, "Meta Learning in Decentralized Neural Networks Through the Lens of Global Workspace Theory", an invited talk at MBZUAI and RIKEN-AIP Joint Workshop on Intelligent Systems
- Feb 2023, "Meta Learning in Decentralized Neural Networks Through the Lens of Global Workspace Theory", an invited talk at Victoria University of Wellington
- Nov 2022, "Meta Learning and Modularity Towards Systematic Generalization", an inner group talk at the MIT Department of Brain and Cognitive Sciences
- Mar 2021, "Segmented Federated Learning", an invited talk at Workshop on Algorithm and Big Data, Transdisciplinary Information Sciences conferences

Academic Services

- Reviewer: IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Artificial Intelligence, Neural Networks, Engineering Applications of Artificial Intelligence, ACM Multimedia, NeurIPS, CVPR, ICML, IJCNN, ACML, AISTATS
- Volunteer for NeurIPS 2021, ICLR 2023
- Organizer for the 1st NeuroAI Social at ICML 2023, the 2nd NeuroAI Social at NeurIPS 2023