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 and Communication Engineering GPA: 4.0/4.0 — 04-2021 ~ 03-2024 (anticipated)

M.E., 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: Federated Learning, Neural Networks

Post-Graduate Research Program, Graduate School of Information Science and Technology — 10-2018 ~ 03-2019
Research Focus: Computer Vision

North China Electric Power University — Beijing, China

B.E., Computer Science and Technology — 09-2014 ~ 08-2018
Thesis: An Attack 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: emergent computations within distributed neural circuits, underactuated robotics, blockchain lab

University of Pennsylvania — Philadelphia, PA, US

Visiting Student — 08-2019 ~ 10-2019

Waseda University — Tokyo, Japan

Visiting Student — 10-2016 ~ 08-2017

EMPLOYMENT

Japan Society for the Promotion of Science (JSPS) — Tokyo, Japan

Research Fellow DC — 04-2022 ~ Present
The principal investor to lead the project of Multimodal Machine Learning in Ambient Intelligence

The University of Tokyo — Tokyo, Japan

Research Assistant, Decentralized AI Lab — 05-2020 ~ Present
Lead the project of Effective Knowledge Transfer for Decentralized Deep Learning

RIKEN Center for Advanced Intelligence Project (AIP) — Tokyo, Japan

Junior Research Associate, AI Security and Privacy Team — 04-2021 ~ Present
RIKEN AIP Center was launched for the Advanced Integrated Intelligence Platform Project of the Ministry of Education, Culture, Sports, Science and Technology (MEXT)
- *Perform research and surveys on Model Poisoning Attacks on Neural Networks, especially in Federated Learning and Multimodal Learning*

United Nations University Headquarters — Tokyo, Japan

Systems Engineer Intern, Computing Centre — 05-2019 ~ 07-2019
The United Nations University is the academic and research arm of the United Nations
- Applied deep neural networks to network intrusion detection for Cybersecurity

Consultant, Computing Centre 05-2021 ~ Present

- Provide expertise in Machine Learning for a project of privacy-preserving phishing detection

- Develop a web application for interactive message inspection with federated learning and natural language processing

RESEARCH GRANTS

Grant-in-Aid for JSPS Fellows, Japan Society for the Promotion of Science (JSPS) 04-2022 ~ 03-2024
Responsibility: Principal Investigator
Project: Trustworthy distributed artificial intelligence for large-scale IoT data knowledge acquisition

SPRING GX Program, Japan Science and Technology Agency (JST) 10-2021 ~ 03-2022
Responsibility: Principal Investigator
Project: Knowledge alignment to improve the generality of decentralized deep learning

SELECTED PUBLICATIONS

Journals

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. 10.1109/TAI.2021.3133819. 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, Ng Chong, and Hideya Ochiai. Information Stealing in Federated Learning Systems Based on Generative Adversarial Networks. *IEEE International Conference on Systems, Man, and Cybernetics. 2021.*

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.*

Yuwei Sun, Nagul Cooharojananone, and Hideya Ochiai. Aircraft Detection Based on Saliency Map and Convolution Neural Network. *IEEE International Conference on International Computer Science and Engineering Conference. 2019.*

HONORS AND AWARDS

- Heiwa Nakajima Foundation Scholarship (one year) 04-2021
- Department Chair's Award for Outstanding Master's Thesis, The University of Tokyo 03-2021
- International Student Scholarship, The University of Tokyo 10-2019
- Excellent Student Scholarship, North China Electric Power University 12-2016
- Mathematical Contest in Modeling Successful Participant, Consortium for Mathematics and Its Applications (COMAP) 12-2015

SKILLS

Programming: Python (Advanced), PyTorch (Advanced), Tensorflow (Advanced), OpenCV (Advanced), SQL (Intermediate), Linux commands (Intermediate), C++ (Intermediate), Java (Intermediate), HTML (Elementary), Git (Elementary), Docker (Elementary), JavaScript (Elementary)
Languages: Chinese (native), English (TOEFL IBT 101), Japanese (JLPT N1 169)
Certification: Deep Learning for Engineer Certification, Japan Deep Learning Association (09-2018)

OTHER ACTIVITIES

Reviewer
Journals: IEEE Transactions on Industrial Informatics, IEEE Transactions on Intelligent Transportation Systems, IEEE Network, Digital Communications and Networks

Conferences: ACM Multimedia, AISTATS, ECMLPKDD, IJCNN, FUZZ-IEEE, IEEE CEC, CVPR Workshop, NeurIPS Workshops, Computing Conference

Invited Talk
"Segmented Federated Learning". Workshop on Algorithm and Big Data, Transdisciplinary Information Sciences Conferences. Online. 03-2021.

Workshops
- AI Governance Workshop. United Nations Office for Disarmament Affairs (02-2021)
- AUA Entrepreneurship Initiative Program. International Innovation Center of Tsinghua University (12-2020)
- Global Talent Program. AIESEC (United Nations Economic and Social Council) (03-2018 ~ 09-2018)