YUWEI SUN

ywsun@g.ecc.u-tokyo.ac.jp | +81-8081165839
7 Chome-3-1 Hongo, Bunkyo City, Tokyo 113-8654, Japan
https://yuweisunn.github.io

EDUCATION

The University of Tokyo Tokyo, Japan
Ph.D., Information and Communication Engineering GPA: 4.0/4.0 04-2021 ~ 09-2023 (anticipated)
Thesis Topic: Modular Neural Networks, Interpretability
Supervisors: Hideya Ochiai, Jun Sakuma, Hitoshi Matsubara

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: Meta Learning, AI Security and Privacy

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: 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 (BMM), Underactuated robotics (EECS), Blockchain (Sloan)

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
Doctoral Course Research Fellow 04-2022 ~ Present

RIKEN Center for Advanced Intelligence Project (AIP) 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 and generality of federated learning and multimodal models*

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

United Nations University Tokyo, Japan
Systems Engineer Intern 06-2020 ~ 12-2020
The United Nations University is the academic and research arm of the United Nations
- Performed research on privacy-preserving deep learning for cybersecurity

Consultant 05-2021 ~ 06-2022
- Researched multi-source domain adaptation in federated learning for vision and text data

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. How the Target Matters: Semi-Targeted Model Poisoning Attack on Federated Learning. *IEEE Transactions on Neural Networks and Learning Systems. 2022* (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**, 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, Montreal AI Symposium
- Volunteer for NeurIPS 2021

Doctoral Consortiums

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