YUWEI SUN

ywsun@g.ecc.u-tokyo.ac.jp | +81-08081165839
7 Chome-3-1 Hongo, Bunkyo City, Tokyo 113-8654, Japan

EDUCATION

The University of Tokyo — Tokyo, Japan
Ph.D., Information & Communication Engineering GPA: 4.0/4.0 — 04-2021 ~ Present
M.E., Information & Communication Engineering (with honors) GPA: 3.84/4.0 — 04-2019 ~ 03-2021
Thesis: Network Intrusion Detection Based on Distributed Trustworthy Artificial Intelligence
Honors: Department Chair's Award
Research Focus: Deep learning, Trustworthy AI, Cybersecurity

Post-Graduate Research Program, Graduate School of Information Science & Technology — 10-2018 ~ 03-2019
Research Focus: Deep learning, Cybersecurity

North China Electric Power University — Hebei, China
B.E., Computer Science and Technology — 09-2014 ~ 09-2018
Thesis: An Attack on Deep Learning Systems Based on Generative Adversarial Networks

ADDITIONAL EDUCATION

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
Research Focus: Cognitive science

University of Pennsylvania — Philadelphia, PA, US
English Language Program — 08-2019 ~ 10-2019

Chulalongkorn University — Bangkok, Thailand
Visiting Student, Department of Mathematics and Computer Science — 02-2019 ~ 03-2019
Research Focus: Computer vision

Waseda University — Tokyo, Japan
Japanese Language Program — 10-2016 ~ 08-2017

EMPLOYMENT

RIKEN Center for Advanced Intelligence Project — 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 (AIP) of the Ministry of Education, Culture, Sports, Science and Technology (MEXT)
Research Focus: Backdoor attacks and its defenses in decentralized deep learning

United Nations University — Tokyo, Japan
Systems Engineer Intern, Campus Computing Centre — 05-2019 ~ 12-2020
Campus Computing Centre manages the University's information and communication infrastructure
- *Developed a deep learning-based network inspection algorithm and extended it to decentralized systems for privacy-preserving machine learning*

Consultant, Campus Computing Centre — 05-2021 ~ Present
Research Focus: Federated learning, Natural language processing

Value Bridge (AIESEC Global Talent) — Tokyo, Japan
Software Engineer Intern, ICT Department — 03-2018 ~ 09-2018
- *Researched and developed an automatic product quality inspection systems based on cloud computing platforms*

PUBLICATIONS

Journal

Yuwei Sun, Hideya Ochiai, 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.*

International Conferences

Yuwei Sun, Ng Chong, Hideya Ochiai. Information Stealing in Federated Learning Systems Based on Generative Adversarial Networks. *IEEE International Conference on Systems, Man, and Cybernetics (SMC). 2021.* (Accepted)

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Intrusion Measurement and Detection in LAN Using Protocol-Wise Associative Memory. *IEEE International Conference on AI in information and communication (ICAIIC). 2021.*

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Deep Learning-Based Anomaly Detection in LAN from Raw Network Traffic Measurement. *IEEE International Conference on Information Sciences and Systems (CISS). 2021.*

Yuwei Sun, Ng Chong, Hideya Ochiai. Network Flows-Based Malware Detection Using a Combined Approach of Crawling and Deep Learning. *IEEE International Conference on Communications (ICC): Next-Generation Networking and Internet Symposium. 2021.*

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Blockchain-Based Federated Learning Against End-Point Adversarial Data Corruption. *IEEE International Conference on Machine Learning and Applications (ICMLA). 2020.*

Yuwei Sun and Hideya Ochiai. Trajectory Optimization for an Autonomous Vehicle Driving Across Stochastic Traffic Flows Based on Direct Collocation. *IEEE International Conference on Control, Automation and Diagnosis (ICCAD). 2020.*

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Visual Analytics for Anomaly Classification in LAN Based on Deep Convolutional Neural Network. *IEEE International Conference on Informatics, Electronics and Vision (ICIEV). 2020.*

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs. *IEEE International Joint Conference on Neural Networks (IJCNN). 2020.*

Yuwei Sun, Ng Chong, Hideya Ochiai. Text-Based Malicious Domain Names Detection Based on Variational Autoencoder And Supervised Learning. *IEEE International Conference on Information Sciences and Systems (CISS). 2020.*

Yuwei Sun, Hideya Ochiai, Hiroshi Esaki. Detection and Classification of Network Events in LAN Using CNN. *IEEE International Conference on International Conference on Information Technology (InCIT). 2019.*

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

INVITED TALKS

- "Segmented Federated Learning". Workshop on Algorithm and Big Data, Transdisciplinary Information Sciences Conferences. Online. 03-2021
- "Cyber Security - Visualizing Malware Behavior". Workshop on UniNet Network and Computer Application, Thailand Ministry of Higher Education. Thailand. 01-2020

HONORS AND AWARDS

- 2022 Japan Society for the Promotion of Science (JSPS) Research Fellow DC 09-2021
- Heiwa Nakajima Foundation Scholarship 04-2021
- The University of Tokyo, Department Chair's Award for Outstanding Master's Thesis 03-2021
- The University of Tokyo, International Student Scholarship 10-2019
- North China Electric Power University, Excellent Student Scholarship 12-2016
- Consortium for Mathematics and Its Applications (COMAP), Mathematical Contest In Modeling, Successful Participant 12-2015

SKILLS

Programming: Python (Advanced), Tensorflow (Intermediate), PyTorch (Intermediate), OpenCV (Intermediate), SQL (Intermediate), Linux commands (Intermediate), C++ (Intermediate), Java (Elementary), HTML (Elementary), Git (Elementary), Docker (Elementary), JavaScript (Elementary)
Platforms: Microsoft Azure (Elementary), Amazon Web Services (Elementary), Google Cloud Platform (Elementary)
Languages: Chinese (native), English (TOEFL IBT 101), Japanese (N1 169)
Certifications: Japan Deep Learning Association (JDLA)

- Deep Learning for General Certification (11-2018)
- Deep Learning for Engineer Certification (09-2018)

OTHER ACTIVITIES

- Program committee member and reviewer for ML4H: Machine Learning for Health.
- Reviewer for IEEE Network.
- United Nations Office for Disarmament Affairs, AI Governance Workshop Certificate (02-2021)
- International Innovation Center of Tsinghua University, AUA Entrepreneurship Initiative Online Program Certificate (12-2020)