DU Linkang

Research Interest: Data Privacy Protection, Trustworthy Machine Learning

Personal Page: linkangd.info

E-mail: linkangd@gmail.com

WeChat: linkangd

Address: Zhejiang University, 38 Zheda Road, Hangzhou, Zhejiang Province, 310027, P. R. China

EDUCATION

Helmholtz Center for Information Security (CISPA) — **Germany, 11/2021–Now**

Research in Trustworthy Machine Learning — Prof. Michael Backes, Dr. Yang Zhang

Zhejiang University, Group of Networked Sensing and Control — **Hangzhou, 09/2018–Now**

Research in Data Privacy Protection — Prof. Peng Cheng

Singapore University of Technology and Design — **Singapore, 02/2018–04/2018**

Research in Encrypted Communications — Prof. David K.Y. Yau

Zhejiang University, College of Control Science and Engineering — **Hangzhou, 09/2014–06/2018**

Major in Automatic Control — GPA: 3.76/4.0 (Top 20%)

RESEARCH OVERVIEW

My research interests are in the intersection of data privacy and trustworthy machine learning. I've published four papers and three Chinese patents related to differential privacy, distributed machine learning, and deep reinforcement learning.

PUBLICATIONS

Data Privacy Protection@*Local Differential Privacy, Maximum Entropy Estimation, Distributed Machine Learning*

- AHEAD: Adaptive Hierarchical Decomposition for Range Query under Local Differential Privacy, **CCS 2021**. **Linkang Du**, Zhikun Zhang, Shaojie Bai, Changchang Liu, Shouling Ji, Peng Cheng, Jiming Chen
- Differential privacy-preserving distributed machine learning, **IEEE 58th Conference on Decision and Control (CDC)**. Xin Wang, Hideaki Ishii, **Linkang Du**, Peng Cheng, Jiming Chen

Trustworthy Machine Learning@*Differential Privacy, Alternating Direction Method of Multipliers, Deep Reinforcement Learning, Hyperparameter Stealing Attack, Backdoor Attack*

- Privacy-preserving distributed machine learning via local randomization and ADMM perturbation, **IEEE Transactions on Signal Processing 2020**. Xin Wang, Hideaki Ishii, **Linkang Du**, Peng Cheng, Jiming Chen
- HyperThief Stealing Hyper-parameters from Deep Reinforcement Learning Models, **USENIX Security 2022 (under review). 1st author**
- Safe Distance is Lost: An Insidious Backdoor Attack in Deep Reinforcement Learning Based Autonomous Driving System, **IEEE Transactions on Information Forensics & Security (under review). 4th author**

Network Intrusion Detection@ *System Invariance Mining, Data-driven Variable Relationship Construction*

- PLC-Sleuth: Detecting and Localizing PLC Intrusions Using Control Invariants, **USENIX RAID 2020**. Zeyu Yang, Liang He, Peng Cheng, Jiming Chen, David KY Yau, **Linkang Du**

STUDENT ACTIVITIES, HONORS AND AWARDS

- Staff in the Student Union of Zhejiang University (2014–2015)
- Chairman in the Student Union of College of Control Science and Engineering (2016–2017)
- Volunteer in the 120th Anniversary of Zhejiang University (2017)
- Volunteer in China Automation Conference (2019)
- China Scholarship Council (CSC) (2021)
- Outstanding Students of Zhejiang University (2015-2021)

SKILLS & INTERESTS

- **Languages**: Chinese (native), English (fluent)
- **Programming**: Python, MATLAB, C/C++ (basic)
- **Interests**: Photography, Badminton, Swimming