Resume

Bo Zhao

Date of Birth：1998.07　　Tel：+86 18652933335

Mail：bozhao@nuaa.edu.cn

Education Background

- 2016.09-2020.06
  Nanjing University of Aeronautics and Astronautics
  Information Security　　Undergraduate　　GPA：3.2/5.0
- 2020.09-
  Nanjing University of Aeronautics and Astronautics
  Cyberspace Security　　Master

Research Interests

- Distributed Machine Learning / Federated Learning Security (ongoing)
- Blockchain and Computationally Intensive Smart Contracts

Ongoing Topic

Distributed Machine Learning / Federated Learning Security

- Advanced poisoning attacks may compromise existing Byzantine-robust federated learning schemes, especially when local datasets are highly non-IID.
- Proposing novel Byzantine-robust federated learning schemes, which could defend local model / local dataset poisoning attacks on highly non-IID local datasets.

Publications

(* marks the corresponding author, red color marks the supervisor.)

- **Bo Zhao**, Peng Sun*, Tao Wang, Keyu Jiang, “FedInv: Byzantine-robust Federated Learning by Inversing Local Model Updates”, AAAI Conference on Artificial Intelligence (**AAAI**), accepted, 2022.
- **Bo Zhao**, Peng Sun, Liming Fang*, Tao Wang, Keyu Jiang, “FedCom: A Byzantine-Robust Local Model Aggregation Rule Using Data Commitment for Federated Learning”, rejected by IEEE Symposium on Security and Privacy (**IEEE S&P**), under revision, 2021.
- **Bo Zhao**, Liming Fang*, Hanyi Zhang, Chunpeng Ge, Weizhi Meng, Liang Liu, Chunhua Su, “Y-DWMS: A Digital Watermark Management System Based on Smart Contracts”, Sensors, accepted, 2019.
- Liming Fang, **Bo Zhao**, Yang Li, Zhe Liu*, Chunpeng Ge, Weizhi Meng, “Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances”, IEEE Network Magazine, accepted, 2020.