Bo Zhao

https://boriszhao.github.io/

Email : bozhao@nuaa.edu.cn
Mobile : +86-186-5293-3335

Education

- **Nanjing University of Aeronautics and Astronautics** — Nanjing, China
  Bachelor of Engineering in Information Security; GPA: 82% — *Sept. 2016 – Jun. 2020*
- **Nanjing University of Aeronautics and Astronautics** — Nanjing, China
  Pursuing Master of Engineering in Cyberspace Security — *Sept. 2020 – Apr. 2023*

Research Experiences

- **Blockchain**: 2017.12 – 2019.12
  - Blockchain and its application; Smart contract design and game analysis; Computational intensive contract; Blockchain based trustworthy distributed machine learning.
- **Federated Learning**: 2020.03 –
  - Trustworthy federated learning **(ongoing)**

Publications

- **Conferences**:
  - (AAAI-22) **Bo Zhao**, Peng Sun*, Tao Wang and Keyu Jiang, "FedInv: Byzantine-Robust Federated Learning by Inversing Local Model Updates," *in Proceedings of the AAAI Conference on Artificial Intelligence*, 2022. (CCF-A, main track oral, accept rate=5%)
  - (ICC-23) **Bo Zhao**, Tao Wang, Liming Fang*, "FedCom: Byzantine-Robust Federated Learning Using Data Commitment," *in Proceedings of the IEEE International Conference on Communications*, 2023. (CCF-C)
  - (ICPADS-22) Tao Wang, **Bo Zhao**, Liming Fang*, "FLForest: Byzantine-robust Federated Learning through Isolated Forest," *in Proceedings of the International Conference on Parallel and Distributed Systems*, 2022. (CCF-C)
- **Journals**:
  - (Sensors) **Bo Zhao**, Liming Fang*, Hanyi Zhang, Chunpeng Ge, Weizhi Meng, Liang Liu and Chunhua Su, "Y-DWMS: A digital watermark management system based on smart contracts," *Sensors*, 2019. (SCI, IF=3.576)
  - (IEEE Network) Liming Fang, **Bo Zhao**, Yang Li, Zhe Liu*, Chunpeng Ge and Weizhi Meng, "Countermeasure based on smart contracts and AI against DoS/DDoS attack in 5G circumstances," *IEEE Network*, 2020. (SCI, IF=10.693)

Projects

- **Self-funding Project**: 2020.01 – , host, ongoing
  - An experimental platform for Byzantine-robust federated learning and poisoning attacks.
  - Integrating mainstream federated learning baselines (FedAvg, Multi-Krum, Zeno, FLTrust, FedGen, several ongoing projects, etc.), and representative poisoning attacks (Back-gradient, Adaptive attack, Badnets, Backdoor FL, etc.).
- **National Key R&D Program of China**: 2021.12 – 2024.11, participant, ongoing
  - Title: "AI Security Defence and Evaluation Technology" (under Grant 2021YFB3100700, RMB 3,000,000).
  - Student leader of federated learning security task force.
- **NUAA Undergraduate Innovation Project**: 2017.12 – 2018.05, principal participant, accomplished
  - Title: "Blockchain based Voting System".
  - Lead to implement a PoW blockchain prototype to record voting logs and make statistics.

Academical Services

- **PC Member**: FL-IJCAI'23
- **Reviewer**: TNNLS, CIKM'23

Awards

- National Scholarship, Ministry of Education, PRC, 2022. (Top 3%)
- First Class Academic Scholarship, NUAA Graduate School, 2020, 2021, 2022. (Top 30%)
- Special Scholarship for Freshmen, NUAA Graduate School, 2020.
- NUAA Outstanding Graduate, NUAA Graduate School, 2023.
- NUAA Outstanding Individual of Research & Innovation, NUAA Graduate School, 2021, 2022.
- NUAA Merit Student, NUAA Graduate School, 2022.