

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

RESEARCH INTERESTS

- **Blockchain System:** 2017.12 – 2019.12
 - Blockchain and its application
 - Game theory based smart contract design
 - Computational intensive contract
 - Blockchain based trustworthy distributed machine learning
- **Artificial Intelligence:** 2020.03 –
 - Byzantine-robust federated learning (**ongoing**)

PUBLICATIONS & ARCHIVES

- **Conferences:**
 - (**AAAI-22**) **Bo Zhao**, Peng Sun*, Tao Wang and Keyu Jiang, “FedInv: Byzantine-Robust Federated Learning by Inverting Local Model Updates,” in *Proceedings of the 36th AAAI Conference on Artificial Intelligence*, 2022. (**Main Track, oral presentation, 5% accept rate**)
- **Journals:**
 - (**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**)
 - (**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**)
- **Archives:**
 - **Bo Zhao**, Peng Sun, Liming Fang*, Tao Wang, Keyu Jiang, “FedCom: A Byzantine-Robust Local Model Aggregation Rule Using Data Commitment for Federated Learning,” *arXiv*, 2021. (Rejected by IEEE Symposium on Security and Privacy 2022, under revision)

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.

AWARDS

- NUAA Top-tier Academic Scholarship 2020, 2021; NUAA Special Scholarship for Fresh Graduate Student; NUAA Outstanding Individual of Research & Innovation 2020;