Qingqian Yang

Shanghai, China — qingqianyang1@gmail.com — (+86) 18888795926

Research Interest: Trustworthy ML, Computer Vision

EDUCATION

Shanghai University of Electric Power, School of Computer Science and Technology — Shanghai, China
M.S in Computer Science — Sep. 2023 — June 2026 (Expected)
GPA: 3.8
Course: Big Data, Theory of Matrices, Blockchain: Principles and Technologies

Hangzhou City University, School of Computer Science and Technology — Hangzhou, China
B.E in Computer Science — Sep. 2018 — June 2022
GPA: 3.8
Course: Computer Network, Machine Learning, Data Structure, Operating System

RESEARCH EXPERIENCE

Adaptive Trigger Injection with Minimal Parameter Adjustment in Federated Learning May 2025 – Present
Instructor: Yang Hua (Queen's University Belfast); Tao Song (Shanghai Jiao Tong University); Hao Wang (Stevens Institute of Technology)

- Improves stealth by adjusting only a small subset of model parameters, leaving the rest of the clean model untouched..
- Enhances attack effectiveness by generating adaptive triggers that better activate the backdoor under varying inputs.

Benchmark of backdoor in Federated Learning. Apr. 2025 — Present
Instructor: Yang Hua, Tao Song, Hao Wang

- The growing diversity of backdoor in federated learning, along with inconsistent experimental settings and FL-specific challenges (e.g., non-IID data, partial participation), hinders fair and reproducible evaluations across studies.
- Developed an extensible benchmark that systematically evaluates representative and recent methods under diverse FL conditions.
  - Includes 10 backdoor attacks and 12 defense mechanisms
  - Supports 5 model architectures and 6 datasets across CV and NLP tasks
  - Includes realistic FL scenarios (e.g., non-IID partitions, varying participation rates, secure aggregation)
- Preliminary results reveal significant inconsistencies in defense robustness under adaptive settings, providing insights into more reliable evaluation practices.

[ICCV 2025] Stealthy Backdoor Attack in Federated Learning via Adaptive Layer-wise Gradient Alignment
Instructor: Yang Hua, Tao Song, Hao Wang — Aug. 2024 — May 2025

- Investigated how to balance the invisible and strength of trigger in FL even under strong defense mechanisms.
- Proposed an adaptive layer-wise gradient alignment strategy to effectively evade various robust detection mechanisms while preserving backdoor strength.
- Only requires **four** additional steps beyond a standard FL backdoor pipeline and is easily integrated into existing FL frameworks to further enhances model effectiveness.
- Extensive evaluations across diverse models and datasets showed that the proposed injection successfully bypasses eight SOTA detection and maintains the trigger impact. Proposed backdoor attack outperforms SOTA methods, with an improvement in backdoor accuracy of up to 54.76%.

PUBLICATION

- Stealthy Backdoor Attack in Federated Learning via Adaptive Layer-wise Gradient Alignment.
  Qingqian Yang, Peishen Yan, Xiaoyu Wu, Jiaru Zhang, Tao Song, Yang Hua, Hao Wang, Liangliang Wang, Haibing Guan (**ICCV 2025**)

- POLAR: Policy-based Layerwise Reinforcement Method for Stealthy Backdoor Attacks in Federated Learning.
  Kuai Yu, Xiaoyu Wu, Linshan Jiang, **Qingqian Yang**, Peishen Yan, Hao Wang, Yang Hua, Tao Song, Haibing Guan

AWARDS

- **National Scholarship** 2025
- **Bronze Medal, International Collegiate Programming Contest (ICPC) Asia-East Continent Final** 2019
- **Graduate Academic Scholarship** 5% according to comprehensive performance. 2023,2024
- **Undergraduate Academic Scholarship** 20% according to comprehensive performance. 2019,2020,2021