
Adversarial Training in Federated Learning
FAT(Federated Adversarial Training) (2020) [23] : Original Idea
Heterogeneous Problems
FedRobust (2020) [101] : Solve Distribution Shifts
Federated Robustness Propagation(2021) [105] : Different Computing Resources
CalFAT (2023) [24] : Skewed Labels Problem
DBFAT (2023) [34] : Decision Boundary
Certified Guarantees
Certifiably Robust Federated Adversarial Learning (2021) [104] : Randomized Smoothing
Adversarial Robustness through Bias Variance Decomposition (2022) [108] : Variance decomposition
Privacy Leakge
FedBVA (2020) [103] : Privacy Protect
Privacy Leakage of Adversarial Training (2022) [106] : Privacy Protect
Slow Convergence
Adversarial Training in Communication Constrained Federated Learning (2021) [107] : Converge Quickly