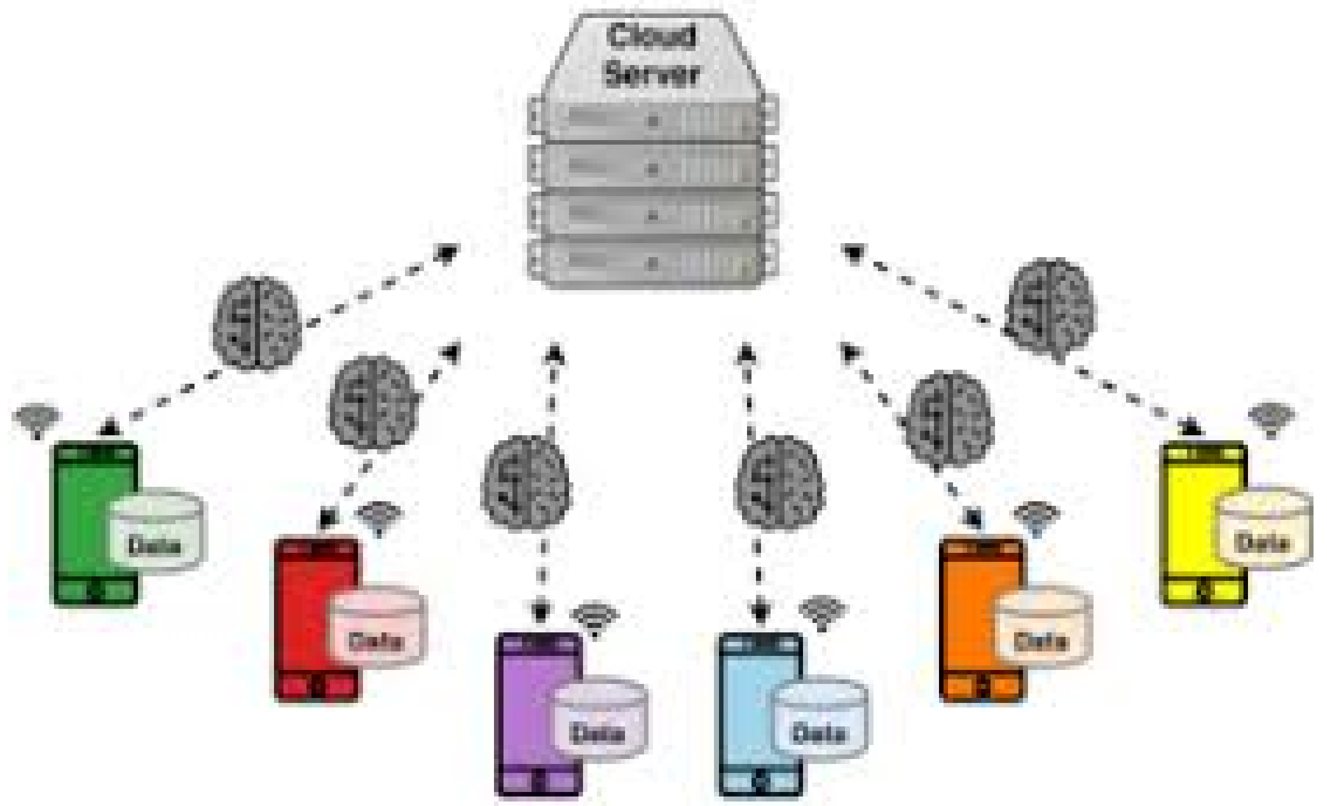
Reliability-Aware Asynchronous Federated Learning (RA-AFL): A Cross-Layer Optimization for Heterogeneous IoFT Networks



BY:
AMMOG WARRIER
GANESH MACHERLA
AMRITAVARSHNI V
MYTHREYEE HARI

Problem Statement

The fundamental problem in the Internet of Federated Things (IoFT) is a critical "System-Algorithm Gap" where idealized AI training protocols fail to account for the physical instability of real-world hardware

The Context:

The Internet of Federated Things (IoFT) involves massive deployment of heterogeneous, battery-constrained devices.

The "Waiting" Problem:

Synchronous FL (FedAvg/FedProx) suffers from the "straggler effect," where the fastest nodes are throttled by the slowest.

The "Context-Blind" Problem:

Current Asynchronous FL (FedBuff/FedAsync) accept updates based on arrival time, ignoring that a "stale" update from a low-battery, overheating node introduces gradient noise and model divergence.

The Mission:

To transition from passive, time-based aggregation to an active, Reliability-Aware framework that optimizes for both mathematical staleness and physical hardware health.

Literature

PAPER	PROBLEMS	SOLUTION	DRAWBACKS	METRICS
Communication-Efficient Learning of Deep Networks from Decentralized Data (FedSGD)	Prohibitive number of updates required for training in federated settings.	FedSGD: Clients compute a single gradient on local data per round ($E=1, B=\infty$).	Extremely high communication overhead. Lacks efficiency from local computation	Achieves baseline model accuracy but requires orders of magnitude more rounds.
Communication-Efficient Learning of Deep Networks from Decentralized Data (FedAvg)	High communication costs and statistical heterogeneity (non-IID data).	FedAvg: Clients perform multiple local SGD updates (E epochs) before model averaging.	Plateaus or diverges with too many local epochs. Requires manual tuning of learning rates.	Reduces communication rounds by 10-100x compared to synchronized SGD.

PAPER	PROBLEMS	SOLUTION	DRAWBACKS	METRICS
Federated Optimization in Heterogeneous Networks Proceedings of Machine Learning and Systems (MLSys) 2020	Systems heterogeneity (Data parameters) Statistical heterogeneity (non IID data)	FedProx Weighted aggregation of client updates proportional to local data sizes scaled by a constant during global model averaging	No client weighting by device health Designed exclusively for synchronous systems Manual hyperparameter tuning	Improves test accuracy by 22% avg over FedAvg
Federated Learning with Buffered Asynchronous Aggregation Proceedings of the 25th International Conference on Artificial Intelligence and Statistics (AISTATS) 2022	Asynchronous FL cause privacy threats with individual updates	FedBuffer Clients send updates asynchronously until server has K updates after which global model is trained	No client weighting by device health or timestamps of incoming gradients Uniform weighting within buffer ignores data quality/noise	3.3x more efficient than traditional synchronous FL, 2.5x more efficient than traditional asynchronous FL

PAPER	PROBLEMS	SOLUTION	DRAWBACKS	METRICS
Federated Learning with Dynamic Trust Scoring for Unreliable or Adversarial Nodes Journal of Computational Analysis and Applications 2024	Data Poisoning Equal treatment of all participants poisons global model	Dynamic trust scores (0-1) from multi-dimensional metrics Weighted aggregation by trust × data size Exponential moving average updates (α=0.2)	No client weighting by device health Manual hyperparameter tuning Binary inclusion/exclusion does not account for proportional weight decay	Accuracy : 82%
Robust Federated Learning with Attack-Adaptive Aggregation	Vulnerability to model poisoning and backdoor attacks; poor performance of existing defenses on non-IID data.	Attack-Adaptive Aggregation: An attention-based neural network that learns to reweight updates and identify malicious traits in a data-driven fashion.	Requires a small validation test set on the server to train the attention module and simulate attacks.	Achieves near-zero Attack Success Rate (ASR) on CIFAR-10, significantly outperforming Krum and FoolsGold

DYNAMIC AGGREGATOR: RA-AFL ARCHITECTURE

KEY COMPONENTS

Asynchronous Participation: Nodes pull and push models independently to eliminate synchronization bottlenecks.

The Reliability Vector (Ri): Updates include real-time metadata (Hbatt, Htemp, Hcomm) to quantify device and link stability.

Staleness Control: Tracks version lag between download and upload, applying a decay function to weight outdated gradients appropriately.

CORE AGGREGATOR LOGIC

Proactive Self-Healing & Denoising

Predictive Safe-Stop: Uses voltage/temp slopes to ingest partial updates from nodes flagged for imminent failure.

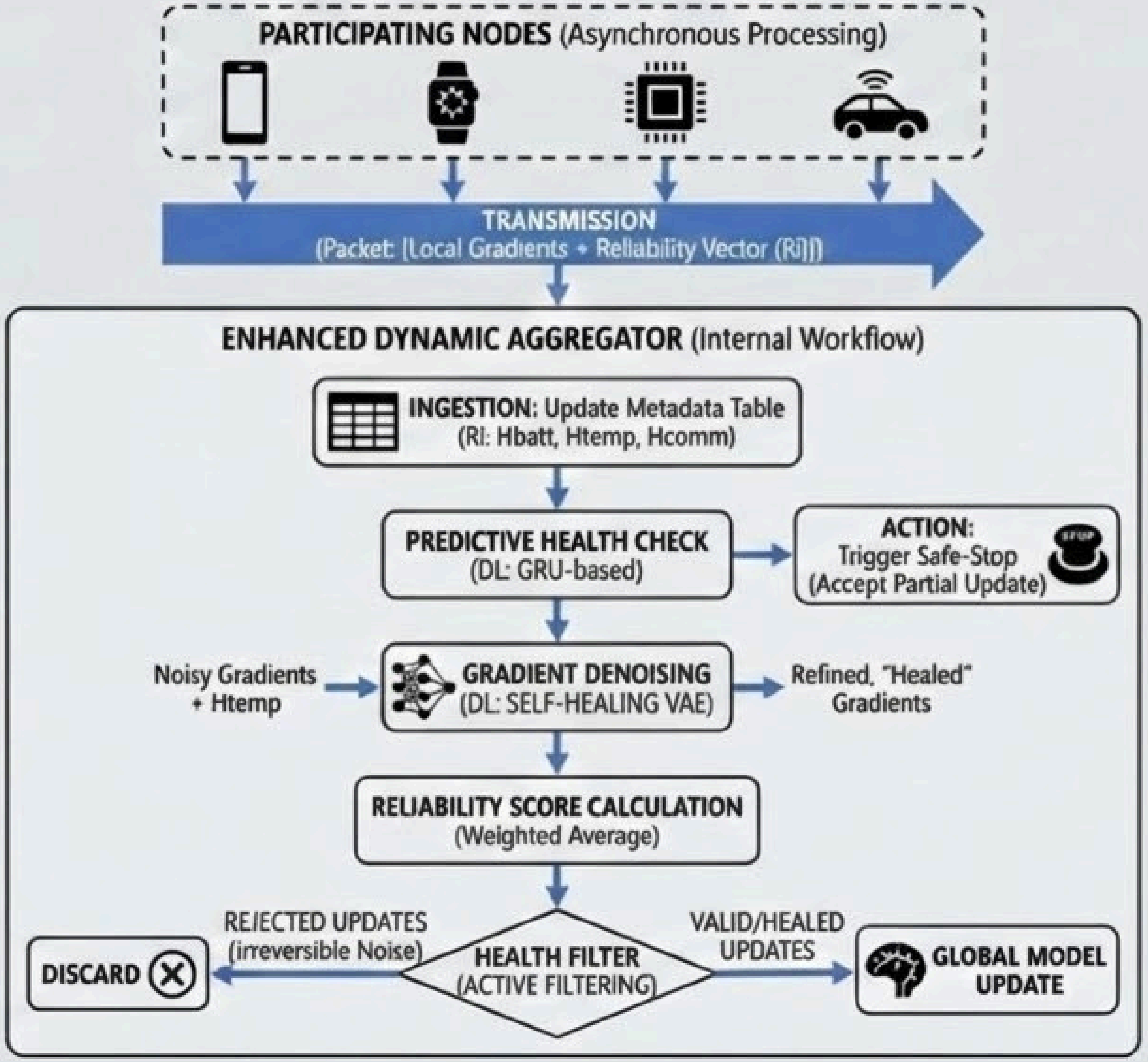
VAE Refinement: A Variational Autoencoder reconstructs "clean" gradients from updates corrupted by thermal jitter or packet loss.

Active Health Filtering

Reliability Scoring: Generates a weighted score (Si) based on DL-predicted stability, telemetry, and staleness.

Dynamic Thresholding: Integrates updates exceeding the reliability threshold into the Global Model while discarding high-noise inputs.

RA-FL ARCHITECTURE DIAGRAM



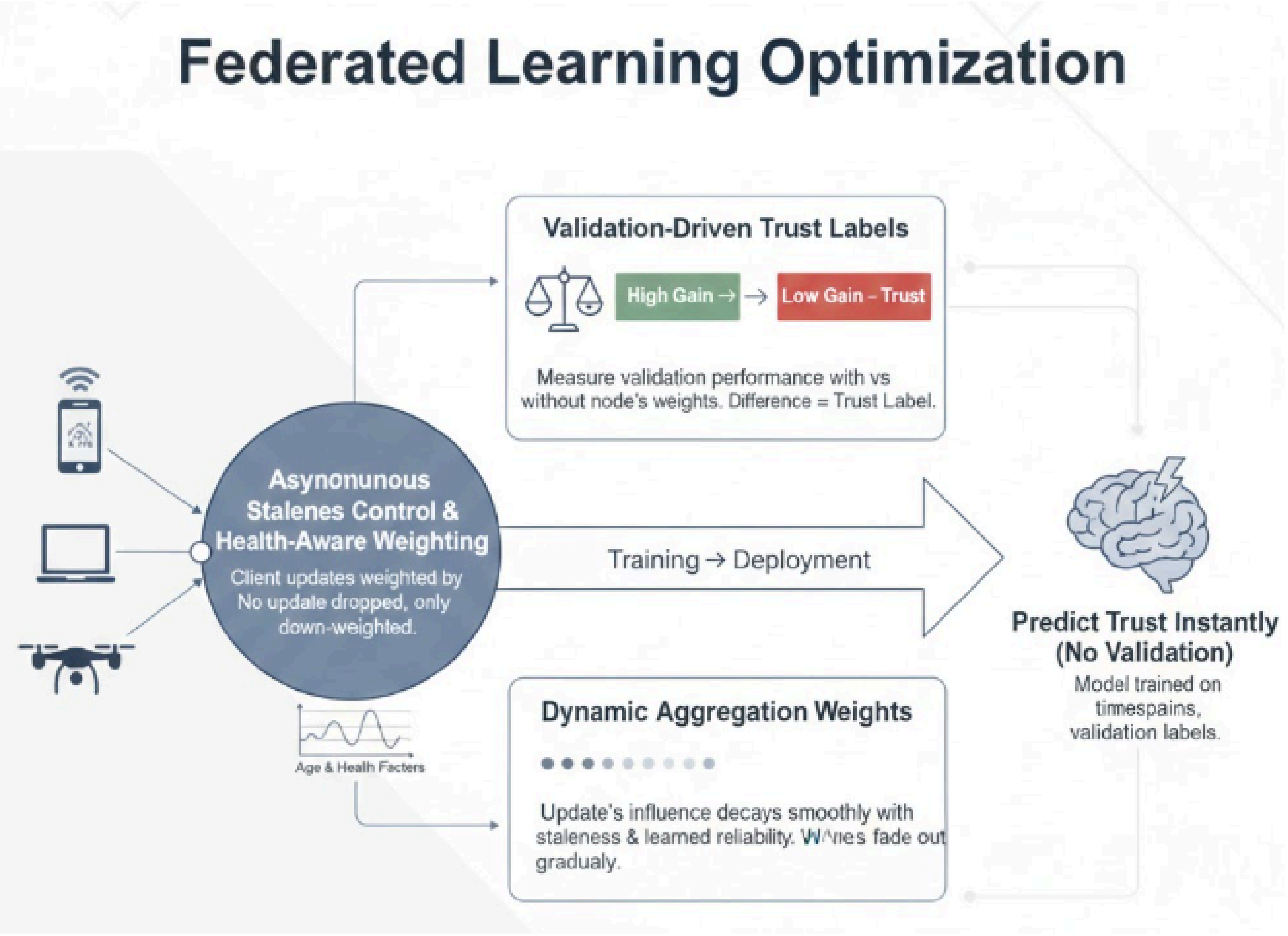
Technical Core - Stateness & Health

Asynchronous Staleness Control & Health-Aware Weighting
Updates are weighted by age and device health; none are dropped, only down-weighted.

Validation-Driven Trust Labels
For each update, we measure validation performance is measured and difference is computed to provide a trust label.

Dynamic Aggregation Weights
Instead of fixed penalties or hard removal, each update fades based on age and reliability, so weak nodes drop off gradually.

Training → Deployment
After training, the model uses health data and timestamps to predict trust instantly without repeated validation.



Comparative Analysis

RA-AFL vs. The State-of-the-Art

Feature	FedProx (State-of-the-Art)	FedBuff (State-of-the-Art)	RA-AFL (Ours)
Feature	FedProx	FedBuff	**RA-AFL** (Ours)
Communication	Synchronous (Slow)	Asynchronous (Fast)	**Asynchronous** (Fast)
Heterogeneity	System-only (Stragglers)	Buffer-only (Staleness)	**Learned Nonlinear Health & Timing Interactions** (Deep Learning)
Update Logic	Proximity Constraint (μ)	First-come, First-served	**Trust Score from Learned DL Model**
Node Chum	Poor (waits for dead nodes)	Moderate (accepts old data)	**High** (filters flaky hardware)
Convergence	Stable but slow	Fast but potentially shakv	**Fast & Stable** with **Performance-Driven Trust**
Deep Learning Integration	None (Standard FedAvg)	Limited (Model updates only)	**Learns Trust** (Health & Time), **Predicts Reliability** (Avoids Validation), **Adapts to Conditions** (Nonlinear)

Experimental Design Design & Expected Results

Simulating Extreme IoFT Environments

- **Environment:** Simulation of 50–100 nodes using a framework like FedScale or Flower.
- **Injected Noise:**
  - **Tier 1:** High-reliability nodes (plugged in, stable Wi-Fi).
  - **Tier 2:** Flaky nodes (simulated battery drain and 20% packet loss).
  - **Tier 3:** Thermal-throttled nodes (simulated noise in gradients due to hardware stress).
- **Key Performance Indicators (KPIs):**
  - **Accuracy vs. Wall-clock Time**: Demonstrating faster convergence than FedProx.
  - **Model Fairness**: Showing that RA-AFL doesn't just ignore slow nodes but integrates them safely.
  - **Robustness**: Stability of the global loss curve despite 30%+ node failure rates.

Conclusion & Future Impact

Towards Scalable and Robust IoFT

Summary:
RA-AFL provides a unified solution to the dual challenges of mathematical staleness and hardware unreliability.

Impact:
This research moves FL toward real-world deployment in "uncontrolled" environments like smart cities, industrial sensor networks, and autonomous drone fleets.

The "Gold Standard":
By integrating hardware metadata into the optimization loop, RA-AFL sets a new benchmark for Cross-Layer Optimization in decentralized AI.

Research and References

- https://eudoxuspress.com/index.php/pub/article/view/4573/3393
- https://arxiv.org/pdf/2102.05257
- https://arxiv.org/pdf/2106.06639
- https://arxiv.org/pdf/1812.06127
- https://arxiv.org/pdf/1602.05629

Thank You!