Fed-DPRoC Dynamic Meta-Layer Aggregation Under Byzantine Attacks on EMNIST

Assignee Research

June 1, 2026

Abstract

This report synthesises findings from 3 peer-reviewed papers addressing the following research question: How does the dynamic meta-layer aggregation approach in Fed-DPRoC compare to other federated learning defense mechanisms (e.g., Krum, Median) in terms of inference accuracy and communication overhead. The rapid growth of Internet of Things (IoT) devices has generated vast amounts of data, leading to the emergence of federated learning as a novel distributed machine learning paradigm. Federated learning enables model training at the edge, leveraging the processing capacity of. 12 claims were extracted from source literature; 9 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.6/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Decentralized Federated Learning on the Edge Over Wireless Mesh Networks. Research question: How does the dynamic meta-layer aggregation approach in Fed-DPRoC compare to other federated learning defense mechanisms (e.g., Krum, Median) in terms of inference accuracy and communication overhead on the EMNIST dataset under Byzantine attacks?.

2 Methodology

Systematic literature search across multiple databases yielded 3 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.6/10.

3 Results

3 papers retrieved. 12 claims extracted; 9 independently verified. Quality review score: 7.6/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Conventional centralized federated learning architecture suffers from a single point of failure.	✓	0.27
Conventional centralized federated learning architecture is susceptible to malicious attacks.	✓	0.20
The study conducts a network performance analysis using stochastic geometry theory.	✓	0.19
The study conducts a network performance analysis using physical interference models.	✓	0.17
System simulations were conducted to assess the decentralized architecture under various network parameters.	✓	0.19
System simulations assessed aggregator methods including FedAvg, Krum, and Median.	×	0.13
The model was trained on the EMNIST dataset.	×	0.12
The EMNIST dataset is used for benchmarking handwritten digit classification.	×	0.14
A compression technique based on genetic algorithms was employed to minimize model size at the edge.	✓	0.20
A compression technique based on genetic algorithms was employed to reduce communication overhead.	✓	0.18
Simulation results show the compressed decentralized architecture achieves performance comparable to the baseline centra	✓	0.25
Simulation results show the compressed decentralized architecture achieves performance comparable to traditional DFL.	✓	0.24

References

- https://doi.org/10.48550/arxiv.2109.04269
- https://doi.org/10.15837/ijccc.2023.6.5890
- https://doi.org/10.1109/access.2023.3329362