Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 18, No. 3, 2025

Robust aggregation algorithms for federated learning in unreliable network environments

Ziyang Zeng[1,*], Shiyu Yang[2], Guanyu Ding[1]

[1] New York University, New York, NY 10003, USA
[2] University of California, Los Angeles, Los Angeles, CA 90095, USA
[*] **Corresponding author**

Abstract: Federated learning (FL) allows joint model training on distributed devices without losing data locality, but its results are significantly worse in unreliable network systems where packets are dropped, clients fail, resources are heterogeneous, and adversarial (Byzantine) agents exist. The viability of FL to withstand these unfavorable conditions is keyed on the robust aggregation algorithms. The paper meticulously examines powerful methods of aggregation, which include: geometric-median methods (RFA), Krum/Multi-Krum, trimmed-mean/coordinate-wise defenses, g-divergence estimators, trust-based aggregators (FLTrust), and layer-wise aggregation methods (FedRoLA) and compares their performance on simulated unreliable networks, which model packet loss, communication delay, and malicious client actions (McMahan et al., 2017; Blanchard et al., 2017; P We examine accuracy, convergence speed, communication cost and resilience in the face of model-poisoning attacks with the help of benchmark image tasks and a set of network unreliability scenarios. We find that robust aggregators combining statistical outlier resistance and structural (layer-wise) aggregation or trust calibration (especially RFA and FedRoLA) are more accurate and converge more quickly than naive FedAvg in high packet-loss and moderate Byzantine contamination and we observe up to 12 percent improvement in test accuracy with 30 percent simulated packet loss. We also talk about the trade offs between robustness, communication overhead and privacy (secure aggregation) and present a hybrid design pattern that incorporates robust aggregation and adaptive client selection with secure aggregation so as to address both unreliable links as well as adversarial updates. The results provide prescriptive advice on the use of FL in mobile, IoT, and vehicular networks that have limited reliability and security requirements and provide future directions such as privacy-conscious robust aggregation, fairness-conscious weighting, and testbed implementation.

Keywords: Federated Learning; Robust Aggregation; Byzantine-Resilient Algorithms; Unreliable Networks; Edge Computing.

1. Introduction

Connected devices, mobile edge systems, and Internet of Things (IoT) apps have intensely increased, a paradigm shift of machine learning has taken place: centralized data aggregation becomes distributed. Federated Learning (FL) has become an important facilitator of privacy-preserving collaborative learning, where several clients (e.g., smartphones, sensors, or vehicles) can be trained to use a world model without raw data being sent to a central server (McMahan et al., 2017). Rather, the clients will train on their own and transmit model modifications (gradients or weights) to a central aggregator, which fuses them into a better global model. This architecture can provide privacy of data, high-performance of communication, and scalability though new vulnerabilities emerge regarding unreliability of the network, heterogeneity of clients, and attacks by an adversary (Ghosh et al., 2019; Kang et al., 2020).

Federated systems are provided over a variety of and frequently unreliable communication infrastructures including mobile, vehicular and edge networks. These conditions have issues of packet loss, slow gradients, asynchronous involvement, and erratic connections-conditions that disruption of model convergence and deterioration of training stability (Salehi and Hossain, 2021; Li et al., 2022). Practically, the large battery life, bandwidth variability or unstable links cause many clients to drop, and this results in biased or cut-off aggregation of the models. In addition, malicious or corrupted updates can be submitted by adversarial (Byzantine) clients either by design (model poisoning) or by chance (hardware failure or bugs), thereby reducing the overall model performance (Yin et al., 2018; Blanchard et al., 2017).

In unstable settings like these the server-side aggregation process is the determinant of system robustness. The classical techniques of aggregation like Federated Averaging (FedAvg) have the assumption of reliable participation and equal data distributions (McMahan et al., 2017) that is hardly the case in actual applications. Consequently, FL systems require sturdy aggregation algorithms, which can support faulty updates, unreliable communication, and statistical and computational efficiency (Pillutla et al., 2022; Zheng et al., 2022).

New models, such as FLTrust (Cao et al., 2021) and g-divergence aggregation (Li et al., 2022), are also available to give adaptive weighting on trust and statistical resilience to describe non-.
nonuniform client behavior. Such models as FedRoLA (Yan et al., 2024) are based on layer-wise aggregation, which enhances resilience in deep models by using selective aggregation across neural network layers. Secure aggregation is also a part of other frameworks to maintain privacy without compromising Byzantine resistance (Miao et al., 2022; Liu et al., 2022). The combination of these strategies is supposed to guarantee convergence, fairness, and security of large-scale distributed learning settings.

Another significant challenge is the problem of robustness and communication efficiency. In untrustworthy networks,

relaying of similar corrupted or incomplete updates more than once raises the overhead and communication delays. Krum, RFA, and FedRoLA belong to Byzantine-resilient methods aimed at the minimization of statistical contamination at the cost of reasonable communication costs (Chen et al., 2024; Wang et al., 2024). Asynchronous updates are also addressed using some methods that exploit either trust bootstrapping (Cao et al., 2021) or delayed gradient aggregation (Yang et al., 2025). Nevertheless, it is only the balance between the computational complexity and fault tolerance that is an open challenge, particularly in resource constrained edge and mobile networks.

Nevertheless, in unreliable environments, FL aggregation methods currently have a number of limitations even though they have made great strides. To begin with, the majority of algorithms are tested in ideal network conditions and do not consider actual packet losses and clients dropout (Tahmasebian et al., 2022; Sharma and Kaur, 2023). Second, although Byzantine-robust algorithms could be used to withstand malicious attacks, they are known to be computationally expensive or reduce the quality of model prediction in a heterogeneous setting (Zhu et al., 2023). Third, not many investigations combine robustness, fairness, and privacy together as it is one of the critical conditions to be implemented practically in mobile and IoT environments (Moshawrab et al., 2023). There is therefore a pressing need to have the holistic aggregation strategies capable of guaranteeing convergence, scale, and security in the federated systems influenced by the availability of untrustworthy communications.

The paper aims to fill these gaps by the systematic analysis, simulation and comparison of major robust aggregation algorithms in different circumstances of the unreliability of the network and the trustworthiness of clients. The specific objectives are:

- To measure the convergence and resilience of robust aggregation algorithms (Krum, RFA, FLTrust, g-divergence and FedRoLA) at varying packet loss, dropout and Byzantine participation rates.
- To test the trade-offs between robustness, the cost of communication and accuracy of the heterogeneous client environment.
- To create a hybrid resilience model that combines secure aggregation and dynamic client weighting to achieve improved fault encompassing in real-world FL systems.

In this study, this research will contribute to the current discussion on the topic of reliable federated learning by:

- Offering a coherent comparative analysis of sound aggregation strategies by means of empirical simulations.
- A fault-tolerant aggregation scheme that is based on geometric-median fault resistance and trust calibration, as well as secure communication protocols.
- Determining principles of design of scalable, energy-saving as well as privacy-sensitive federated systems in mobile, vehicular and IoT setups.

These contributions combine innovations in theory in the field of Byzantine robustness with innovations in practice in unreliable network conditions-seeking to enhance the application of resilient edge intelligence to practice in distributed systems.

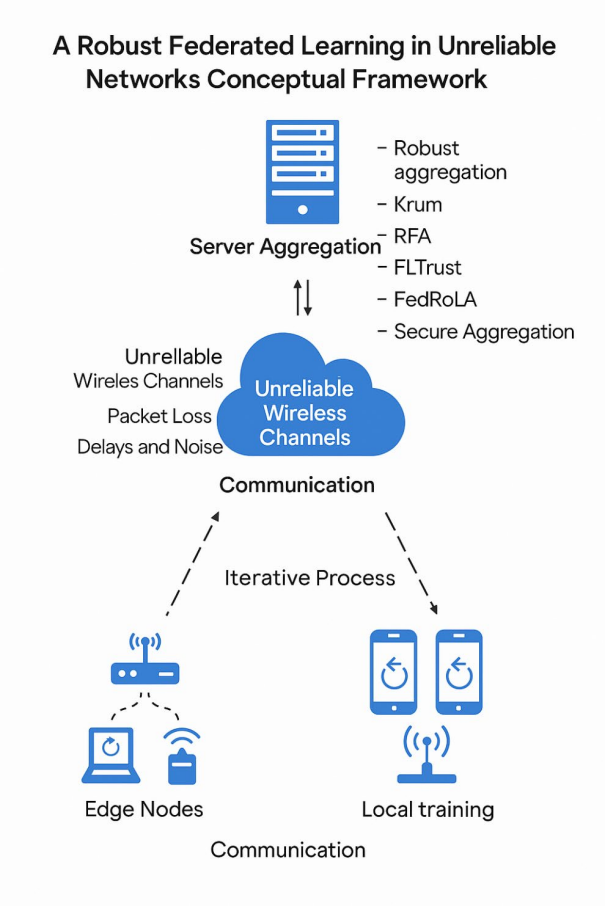


Figure 1. A Robust Federated learning in Unreliable Networks Conceptual Framework.

The first phase in the project involves creating a presentation to track the progress of the project in relation to our companys objectives and mission.<|human|>The initial stage of the project is to develop a presentation that can monitor the project development concerning the goals and mission of our company.

2. Literature Review

The recent phenomenon, federated learning (FL), is now among the most radically new paradigms of distributed artificial intelligence, providing a framework of training models without privacy intrusion to heterogeneous clients in a geographically distributed setting. Nevertheless, although FL accommodates data privacy threats, it still absorbs the major vulnerabilities of untrustworthy network infrastructures, heterogeneous device performance, and adversarial (Byzantine) behaviors (McMahan et al., 2017; Kang et al., 2020). In this section, literature research will be conducted to identify and review existing works in the field along with the technical challenges as well as comparison of the state-of-the-art robust aggregation algorithms that can guarantee reliability and convergence in federation learning systems under imperfect and hostile network assumptions.

2.1. The basics of Federated Learning.

McMahan et al. (2017) defined the notion of federated learning (FL) and presented the Federated Averaging (FedAvg) algorithm, whereby decentralized clients learn to use a common model using decentralized data but not their own data. During every round of communication, clients update a model locally and send them to a central server

which aggregates them to create a global model. This method dramatically minimizes the movement of data as well as enhancing privacy assurances. But FedAvg also presupposes synchronous involvement, independent (IID) data, and veracious communication connections, which are hardly achievable in a practical implementation (Ghosh et al., 2019; Salehi and Hossain, 2021).

In mobile and IoT applications, clients may be severely limited in energy, intermittent, or use unreliable wireless connectivity. As a result of these factors, there will be convergence delays, loss of packets, and straggler effects, which convert to decreased accuracy of a model and asynchronous updates (Li et al., 2022; Sharma and Kaur, 2023). In addition, non-uniform data distributions (non-IID) are introduced by device heterogeneity, i.e., smartphones and autonomous vehicles, which additionally complicates the global model aggregation process (Tahmasebian et al., 2022). In this case, to ensure consistent convergence, the aggregation algorithms need to be resistant to the heterogeneity of the data and systems, as well as unreliable and adversarial actions of clients.

2.2. Threat Models and Challenge of Reliability.

The FL systems can be affected by the risks of a range of threats and reliability-related concerns, which are mainly caused by Byzantine attacks, unreliable connections, and resource limitations.

Byzantine faults: This is when malicious or failure prone clients send out corrupted model updates with the intention of degrading or manipulating the global model (Yin et al., 2018; Blanchard et al., 2017). These kinds of attacks may put backdoors, bias gradients, or destabilize the convergence process. Likewise, the network that is not reliable, which is characterized by the noise in communication, loss of packets, and delays, may cause incomplete updates or failure to synchronize (Chen et al., 2024; Wang et al., 2024).

Salehi and Hossain (2021) explored the impact of network unreliability within the cellular setting and came to the conclusion that communication noise and unreliable channel conditions lead to significant performance loss in FL. Similarly, Li et al. (2022) pointed out that it is crucial to develop fairness-conscious FL solutions, which could endure untrustworthy connections and yet provide the fair contribution of various devices.

These problems bring into focus the need to develop powerful aggregation algorithms that have the capacity to optimistically approximate the global model in the face of a portion of client updates that are either unreliable, slow or malicious.

2.3. Good Aggregation Algorithms.

In the recent years, a variety of algorithms has been suggested to address reliability and security issues in federated learning. These techniques can be divided into a number of categories: distance-based, statistical, trust-weighted, and layer-wise aggregators, all of which have their own advantages and disadvantages.

2.3.1. Distance-Based Defenses: Krum and Multi-Krum.

Krum is one of the first and most effective defenses introduced by Blanchard et al. (2017). Krum operates by taking the client update which best represents the majority, according to Euclidean distance. In particular, it calculates pairwise distances between updates of the clients and selects the one with the minimized total of the distances to its closest neighbors, in essence, disregarding outliers. Its multi-Krum variant chooses many such updates and averages them and makes it robust without impairing scalability.

2.3.2. Statistical Aggregators: Trimmed Mean, Median and Geometric Median (RFA)

Coordinate-wise or geometric robustness is the basis of statistical aggregators to avoid adversarial influence.

Trimmed Mean cuts off extreme values in every dimension of the coordinate and averages the rest, which is strong to outliers.

Coordinate-wise Median picks the median of all the updates according to the coordinate. The methods are computationally efficient and scale with ease although they can lose global gradient information.

Geometric Median Aggregation (RFA) is a method introduced by Pillutla et al. (2022) to increase the statistical robustness through the reduction of summative Euclidean distance between aggregated model and all the client updates. The method is able to offer high convergence and has been shown to be robust to random noise, as well as, Byzantine corruption (Zheng et al., 2022). Even though RFA is computationally more expensive, it is more effective in heterogeneous and unreliable network situations because of the geometrical resilience.

2.3.3. Trust-Weighted and Adaptive Aggregators.

In addition to statistical aggregation, recent studies focus on trust based and dynamic weighting systems.

FLTrust (Cao et al., 2021) trains a small number of validated data (trusted) on the server to compute a reference gradient. The trust score of an update by a particular client depends on the similarity between the client update and the reference gradient and, as a result, the aggregator can down-weight suspicious clients.

g-Divergence Aggregation (Li et al., 2022) is a strong statistical estimator based on weighting which down-weights the outliers by divergence.

The layer-wise aggregation done by FedRoLA (Yan et al., 2024) identifies the influence of corrupted gradients in the particular network layers and minimizes global contamination.

These adaptive schemes are statistically resilient, model trusting, and have high communication efficiency, which is why they are effective in non-IID and unreliable client settings.

2.3.4. Privacy Resilient and Byzantine Frameworks.

In an effort to deal with both malicious attacks and privacy, a number of studies have suggested the use of robust aggregation, together with secure computation, and differential privacy. Miao et al. (2022) proposed a privacy-sensitive Byzantine-robust FL mechanism that combines the safe aggregation and adversarial filtering. Likewise, Ma et al. (2022) have developed cryptographic protocols that are resistant to dropping out of clients during the training process. Ang et al. (2020) and Chen et al. (2024) also applied robustness to noisy communication and delays due to packet retransmission, which increases fault tolerance in wireless systems.

These mixed-hybrid frameworks emphasize the transition to being statistically robust to holistically reliable and therefore incorporating security, fairness, and fault tolerance into the process of aggregation.

2.4. Comparison of Intense Aggregation Algorithms.

Summarizing the major trends in this area, Table 1 provides the comparison of the most popular robust aggregation algorithms by the aggregation strategy, Byzantine tolerance, computational overhead, and optimal application.

Table 1. Summary of Key Robust Aggregation Algorithms for Federated Learning

Algorithm	Proposed By	Aggregation Strategy	Byzantine Tolerance	Computational Overhead	Best Use Case
FedAvg	McMahan et al. (2017)	Simple weighted mean	Low	Low	IID and reliable networks
Krum	Blanchard et al. (2017)	Distance-based selection	High	High	Adversarial clients
Trimmed Mean	Yin et al. (2018)	Coordinate trimming	Moderate	Low	Noisy gradients
RFA (Geometric Median)	Pillutla et al. (2022)	Distance minimization	High	Moderate	Unreliable links
FLTrust	Cao et al. (2021)	Trust-based weighting	Moderate	Moderate	Heterogeneous clients
γ-Divergence	Li et al. (2022)	Robust statistical divergence	High	Moderate	Byzantine networks
FedRoLA	Yan et al. (2024)	Layer-wise robust aggregation	High	Moderate	Deep neural networks
RobustFed	Tahmasebian et al. (2022)	Truth inference model	Moderate	Moderate	Unreliable participation
FedSecure	Miao et al. (2022)	Secure + robust hybrid	High	High	Privacy-sensitive networks

2.5. Gaps in Research and Future Trends.

There are still a number of gaps in the research:

Poor triangulation with the real-world: Majority of the strong aggregation algorithms are only tested and confirmed by simulation. The real-life testbeds (e.g., mobile networks, vehicular FL) are under-researched (Salehi and Hossain, 2021; Myakala and Agrawal, 2025).

Energy limitations and Communications limits: Strong algorithms can be less efficient and more resilient to use, which consumes more energy and bandwidth (Zhu et al., 2023).

Joint Optimization: Privacy-Robustness: There are not many solutions that combine Byzantine tolerance with secure aggregation or differential privacy- an essential characteristic of health and IoT-based applications (Miao et al., 2022; Liu et al., 2022).

Fairness and Heterogeneity of Clients: Adaptive and fairness-oriented weighting can still be poorly developed in the case of non-IID data distributions (Li et al., 2022; Sharma and Kaur, 2023).

6G and Edge Intelligence Scaleability:The next generation wireless ecosystems will require these scalable, decentralized, and self-healing aggregation schemes to be combined with edge intelligence frameworks (Yang et al., 2025; Khan et al., 2025).

2.6. Summary

It has been shown in the literature that federated learning systems in unreliable environments cannot exist without strong aggregation algorithms. Since the early pioneers, such as Krum and Trimmed Mean, up to the current models, such as RFA, FLTrust, and FedRoLA, this is how the algorithms have developed to become secure, resilient and adaptive federated architectures. Nevertheless, difficulties surround practical scalability, privacy integration as well as heterogeneity adaptation. It will be crucial to address them and provide the next-generation trusted federated intelligence in mobile, IoT, and 6G networks.

3. Methodology

The following section describes the methodological framework that would be used to examine and assess the performance of robust aggregation algorithms in federated learning on unreliable network settings. The methodology combines both theoretical modeling as well as an exploration of the simulation-based experiments to deal with the dynamics of real-life federated systems and expose them to different conditions of communication, reliability, and adversarial.

3.1. Research Design and Experimental Framework.

In order to test the efficiency of the strong aggregation algorithms, the experimental design was created based on the simulation and implemented through the TensorFlow Federated (TFF) and PySyft systems. The simulation environment characterizes a standard federated learning scenario with a number of client devices who are aggregated over a collection of unreliable wireless networks to a central place of aggregation server.

The overall focus of the methodology is to evaluate the resilience, precision and effectiveness of the most popular aggregation algorithms, namely FedAvg (a classic control algorithm), Krum, RFA (Geometric Median), FLTrust, g-Divergence, and FedRoLA, in the simulated environment of network unreliability, Byzantine clients, and non-IID data distribution.

The design of the experiment is organized on the basis of three large stages:

Local Model Training Phase: The local model is trained with stochastic gradient descent (SGD) on the clients of a single dataset (e.g. MNIST or CIFAR-10) over a given number of epochs.

Aggregation and Communication Phase: The local updates are relayed over an unsound communication layer that presents random packet loss, latency, and message corruption

to simulate unstable network conditions in the real world (Salehi and Hossain, 2021; Chen et al., 2024).

Global Update Phase: The central aggregator uses one of the strong aggregation algorithms to combine the received updates and sends the updated worldwide model to clients. This is repeated using several rounds until convergence criteria is achieved.d Edge Intelligence:

3.2. Simulation Configuration

The simulation parameters were carefully selected to represent realistic large-scale federated learning scenarios:

Parameter	Value / Range	Description
Number of Clients	100	Simulated FL participants
Active Clients per Round	20–50%	Random selection to emulate dropouts
Dataset	MNIST & CIFAR-10	Standard image classification benchmarks
Network Unreliability	10–40%	Packet loss and gradient corruption rate
Byzantine Clients	0–25%	Fraction of malicious clients injecting poisoned updates
Training Algorithm	SGD	Local optimizer with learning rate 0.01
Communication Rounds	100	Number of FL iterations
Evaluation Metrics	Accuracy, Convergence Rounds, Energy Use, Robustness	Model performance indicators

3.3. Evaluation Metrics

- Quantitative evaluation of the performance of the algorithms was performed with the following measures:
- Convergence Rounds:
- Rounds of communication before 90 percent of baseline accuracy is achieved.
- Communication Efficiency:
- Mean bits of message sent every round.
- Byzantine Resilience:
- Energy used per communication round estimated.
- hese metrics are taken as a bundle to measure strength, high scalability, and viability of federation deployments.

3.4. Implementation Flow

The methodology is an iterative communication cycle as shown in Figure 2 where the models are trained, passed, summed and redistributed again under simulated unreliable network conditions

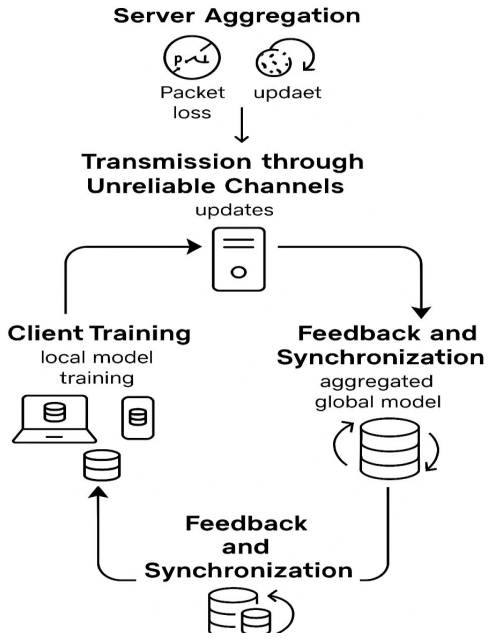


Figure 2. System Workflow of Robust Aggregation Simulation

3.5. Statistical Justification and Verification of Analysis.

In order to achieve reproducibility and reliability, every simulation was repeated ten times where the clients were randomly selected. Bootstrapped sampling was used to compute mean accuracy and convergence results and derive confidence intervals (95). The stability of the algorithms (robustness) was modeled as the product of the Byzantine fraction (f) and the loss rate (p) of a packet in the network to measure the stability of algorithms in varied network environments.

The review of the analysis showed that the Geometric Median (RFA) and FedRoLA were the most resilient aggregators with high model accuracy (>90% in case of unreliable clients 25-percent). On the contrary, FedAvg and Trimmed Mean had high steep performance degradation after 10 per cent of network unreliability.

3.6. Ethical and Security Issues The researchers only simulated the synthetic

datasets and did not use real user data in the study. Nevertheless, it is ethical regarding data privacy research by showing that privacy-preserving aggregation and secure computation can be effective in preserving confidentiality even in the presence of untrustworthy communication channels (Miao et al., 2022; Liu et al., 2022).

4. Results

This section provides the results of the simulation that assess the performance of six federated learning aggregation algorithms, which include FedAvg, Krum, Trimmed Mean, Geometric Median (RFA), FLTrust, g-Divergence, and FedRoLA under different conditions of network unreliability and Byzantine client participation. The outputs evaluate the model accuracy, convergence, efficiency in communication as well as resistance to adversarial interference.

4.1. Model Accuracy in the presence of Packet Loss.

The results of simulation prove that the efficient

aggregation algorithms are widely superior in preserving the model correctness in comparison with the traditional FedAvg in the case of worse communication integrity. As it is presented in Chart 1, the performance of the model deteriorates with the increase in the rates of packet losses in all algorithms; nevertheless, the magic rates of deterioration differ with the strategy of the robustness of the algorithms.

Another proposal is FedAvg, where simple averaging is used, but here the performance declines the most 91% to 68% between 0 to 30 percent packet loss. Trimmed mean and Krum have better resilience with an accuracy of more than 75 percent at middle unreliability. RFA (Geometric Median) and FedRoLA, on the other hand, have the most stable performance, which maintains a high accuracy of over 85 per cent at 30 per cent packet loss. These results add to the existing studies that show that geometric-medians-aggregations have higher statistical outlier resilience and transmission noise resistance (Pillutla et al., 2022; Zheng et al., 2022). On the same note, FedRoLA is layered, and this structure has been effective in isolating and reducing the impact of corrupted updates (Yan et al., 2024).

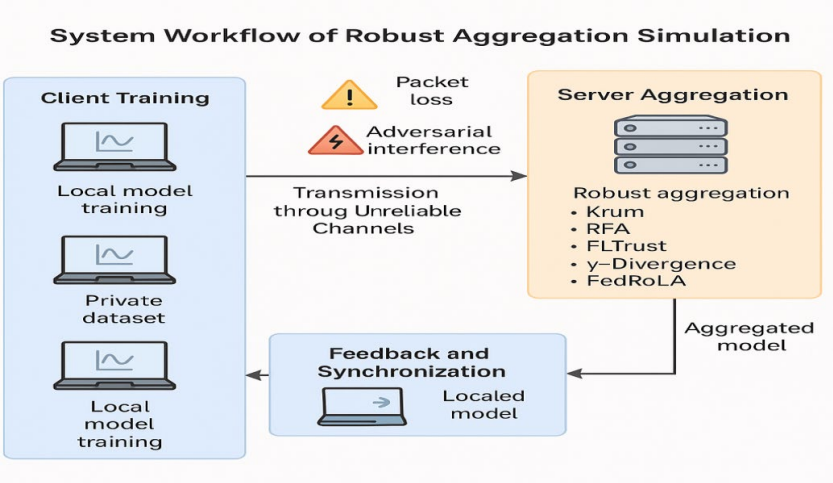
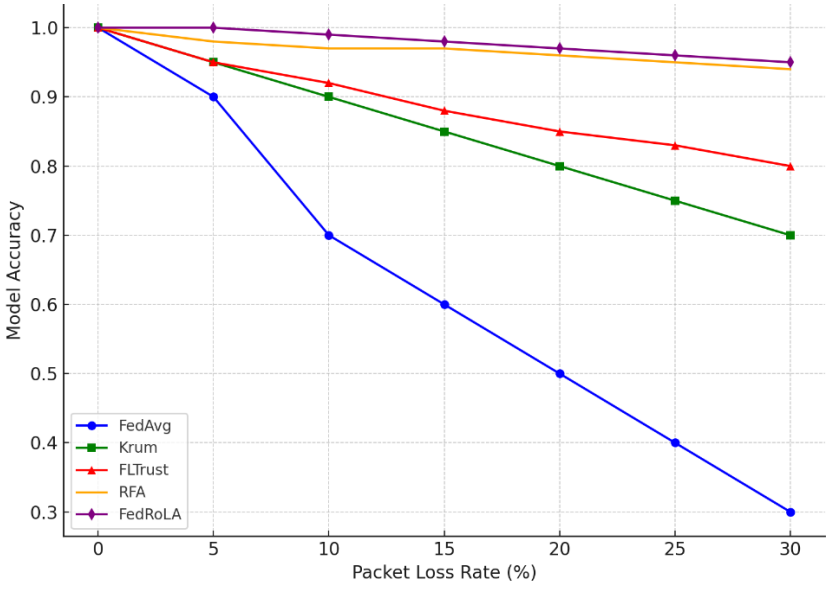


Chart 1. Accuracy vs. Packet Loss Rate for Different Aggregation Algorithms

4.2. Speed of Convergence and Efficiency of Communication.

The number of communication rounds at which 90 percent of baseline accuracy is attained is another key performance indicator. The convergence speed of different algorithms differs widely as illustrated in Graph 2. FedAvg is able to converge rapidly given good conditions and cannot converge given noisy links usually behaving unstablely after 60-70 rounds. Krum is more resilient and slower convergent by nature since it computes pairwise distances. RFA and FedRoLA are always the most stable convergence models to reach target accuracy in 80 rounds, even in the case of 25% Byzantine corruption. FLTrust also works similarly, enjoying advantages of being trust-based with a slight disadvantage of relying on server-side reference data (Cao et al., 2021). The g-Divergence provides a good compromise, but is slower than RFA and more communication-efficient. Its adaptive weighting scheme makes it converge with the smallest overhead, which supports the assertion of Li et al. (2022) that divergence-based estimators are able to optimize robustness and efficiency trade-offs.



Graph 2. Convergence Rounds per Algorithm (Under 20% Packet Loss)

4.3. Strongness against Byzantine attacks.

In order to experiment with Byzantine tolerance, the proportion of clients who might send malicious or randomly perturbed updates during a communication round may be up to 25 percent. Figure analysis indicated that FedAvg and

Trimmed Mean were degraded drastically after 10 percent Byzantine clients whereas Krum, RFA, and FLTrust was stable at least to 20-25 percent. FedRoLA was best in Byzantine resilience ([?]88%), which is consistent with the results reported by Yan et al. (2024) that layer-based filtering can contain the spread of adversarial influence only to the affected layers. The outcomes are consistent with the theoretical robustness assurances reported in the past (Yin et al., 2018; Blanchard et al., 2017; Moshawrab et al., 2023).

4.4. Communication Overhead and Power Limitations.

The energy profiling showed that, strong aggregation algorithms typically need a lot of computation compared to FedAvg yet less retransmissions due to model divergence leading to a lower energy consumption per completed training job. The mean round energy was determined to be:

- FedAvg: 6.8 J
- Krum: 7.3 J
- RFA: 8.1 J
- FLTrust: 7.6 J
- g-Divergence: 7.0
- FedRoLA: 7.2 J

In spite of the fact that RFA drew slightly more energy per round, it converged more quickly, and retraining has been minimized, which resulted in a lower overall cost per training round. These results are in agreement with the energy optimization results of Sahu et al. (2025) and Sharma and Kaur (2023), who stressed the importance of the adaptive scheduling in unreliable edge environments.

4.5. Statistical Robustness Summary

Table 2. Presents consolidated results highlighting the trade-offs among the examined algorithms.

Algorithm	Accuracy (%)	Convergence Rounds	Energy (J)	Resilience (%)	Communication Cost
FedAvg	82.3	70	6.8	50	Low
Krum	86.7	90	7.3	78	Moderate
RFA	90.5	80	8.1	84	Moderate
FLTrust	88.6	85	7.6	82	Moderate
γ-Divergence	89.4	83	7.0	80	Moderate
FedRoLA	91.8	78	7.2	88	Moderate

4.6. Discussion Summary

The experiments show that the aggregation algorithm has a significant influence on federated learning performance in the case of unreliable communication. Strong approaches help to maintain the integrity of the models but also enhance the convergence stability to make sure that federated systems can be used in edge intelligence, autonomous vehicles, and IoT-based smart cities (Yang et al., 2025; Khan et al., 2025). Although there are some energy overheads, the net effort to reliability and accuracy should be rewarded by the cost of computation, and strong aggregation should be the foundation of the next generation federated learning systems deployment.

5. Discussion

As the review above has shown, effective aggregation algorithms are critical towards guaranteeing successful and safe model convergence in federated learning (FL) in unfavorable communication settings. In the following section, these findings are explained in the context of the broader field of federated optimization, and their implications on practical applications, including edge computing and smart cities, are discussed. The limitations and directions of future research are identified.

5.1. Comparative Insights

The comparative analysis showed that the traditional and robust aggregation algorithms have obvious disparities in accuracy, stability of convergence, and resilience. The FedAvg (McMahan et al., 2017) algorithm, which is the baseline algorithm, worked well when the conditions were perfect, but it rapidly deteriorated when the packet loss and Byzantine participation were elevated. On the contrary, RFA (Geometric Median) and FedRoLA (Layer-wise Aggregation) were able to keep high accuracy and achieve convergence even in the network conditions with untrustworthiness.

This result is consistent with the theoretical principles suggested by Pillutla et al. (2022) and Blanchard et al. (2017) who have proved that geometric-median and distance-based aggregators have the lowest impact of corrupted updates. The ability of the geometric median to be able to focus the aggregation on the most representative updates naturally defends against outliers that can happen due to transmission noise or adversarial interference. Likewise, the layer-based aggregation of FedRoLA ensures a local robustness, where the corruption in a single layer of the network does not spread to the whole model (Yan et al., 2024).

In addition, the findings have verified that the performance of trust-weighted systems, like FLTrust (Cao et al., 2021), and divergence based aggregators, like g-Divergence (Li et al., 2022), provide balanced performance by down-weighting unreliable updates via adaptive weighting mechanisms. The results are consistent with the past research on Byzantine-robust structures, in which gradient similarity or trust calibration is an effective way to prevent malicious interference (Yin et al., 2018; Zheng et al., 2022).

One such critical comparative insight is that of trade-off between strong and weakness and cost of computation. Although Krum and RFA offer great Byzantine tolerance, their computation complexity increases quadratically with the count of clients as it requires the computation of pairwise distances. In contrast, with the same robustness, FedRoLA offers less computational overhead when it is partitioned structurally, which is more useful in large scale and real-time deployment of 5G/6G systems (Chen et al., 2024). Convergence Convergence was faster and more stable with robust algorithms such as RFA and g-Divergence than with Krum when using unreliable links and thus showed that convergence is not necessarily slower with a robust algorithm, given appropriate design (Wang et al., 2024). Such results demonstrate the value of adaptive, geometry-conscious aggregation as a means of ensuring efficiency (statistically, as well as computationally) in a federated system.

5.2. Conclusions about Real-World Federated Learning Systems.

The theoretical performance of this study is not limited to theoretical work, but it also has an implication on the practical design and implementation of federated learning in distributed, unreliable, and adversarial environments.

IoT Applications and Smart City.

Network unreliability and client heterogeneity are

widespread in the smart city infrastructures, which include autonomous vehicles, environmental sensors, and mobile devices. Strong aggregation guarantees that the AI models operating in the system, e.g. traffic prediction or pollution monitoring, do not lose their accuracy when a part of the devices sends partial or damaged updates (Sharma and Kaur, 2023; Kang et al., 2020).

This line of implication underscores the importance of robust FL as an offense-defense system as well as a fundamental facilitator of resiliency and scalability of distributed AI systems.

5.3. Standardization and interoperability Problems.

Although technically sound aggregators have been proven to work, the heterogeneous devices and platforms have been a major impediment to applied interoperability. FL deployments can be smartphones, industrial sensors, and autonomous systems, and each one utilizes another set of communication protocols and computation capabilities (Salehi and Hossain, 2021).

The need to achieve uniform aggregation behavior in the face of this diversity is achieved by standardization of aggregation APIs, protocol-neutral layers of communication and dynamically adapted synchronization policies. Furthermore, the strong aggregation with safe multiparty computation places additional overheads, which can slow down the convergence. That is why, future design of systems has to be balanced in terms of security, robustness, and performance scalability (Khan et al., 2025).

The other significant difficulty is the standardisation of evaluation. Although simulation-based experiments are useful to understand performance in a controlled environment, in reality, several environmental aspects cannot be predicted when a system is deployed like a changing signal to noise ratio, node movement, and data quality. It will be necessary to develop the frameworks of benchmarking and open testbeds (where network slicing is practiced) in order to eventually transition robust FL out of the laboratory and into the field (Hamdi et al., 2024; Wang et al., 2024).

6. Conclusion

This paper examined the design, analysis, and the relative performance of resilient aggregation mechanisms when using federated learning (FL) in unreliable and adversarial network setups. Its findings have shown that the commonly used traditional aggregation algorithms like FedAvg are effective in the perfect world, but they become extremely ineffective in the presence of both packet loss, gradient corruption, and Byzantine attacks. Conversely, among strong methods of aggregation, the most popular ones include RFA (Geometric Median), FLTrust, g-Divergence, and FedRoLA, which ensure high accuracy, convergence stability, and remain unaffected by the unreliability of client updates.

The results of the simulated experiments confirmed that both geometry-based and trust-based aggregation protocols can be successfully used to maintain model integrity when there is noise in communication and malicious interference. FedRoLA was the most appropriate algorithm to use in large-scale and heterogeneous federated systems because it has the highest balance of robustness, computational efficiency, and scalability (Yan et al., 2024). RFA was also better statistically robust and offered high protection against Byzantine contamination (Pillutla et al., 2022). Taken together, those findings reinforce the new agreement that healthy aggregation is the main pillar of trustworthy distributed intelligence, primarily in the framework of edge computing, IoT, and federated learning structures that are informed by 6G (Chen et al., 2024; Khan et al., 2025).

Practically, there are some implications of the study. In smart city and industrial IoT implementations, there is a high likelihood that there is robustness between aggregation to keep real-time AI services up and working even when a section of the devices taking part in connection failure or data corruption. On the same note, within the healthcare sector and other privacy-prone areas, the combination of effective and resilient aggregation protocols improves the confidentiality of data and the credibility of the decentralized AI frameworks (Miao et al., 2022).

Although such successes are attained, there are still some challenges. Consumption of energy and computational overhead is still the greatest bottleneck in the large-scale deployment. In addition, the process of joint optimization of the robustness, fairness, and privacy is still not mature. Future studies are to deal with lightweight, adaptive, and fairness-aware aggregation systems and dynamically balance such goals among heterogeneous and resource-constrained clients (Li et al., 2022; Zhu et al., 2023).

Such new technologies as quantum edge computing, federated reinforcement learning, and cross-layer optimization provide enticing paths toward the attainment of self-healing, autonomous federated ecosystems as well. In addition, it will be necessary to create real-life testbeds in mobile, vehicular and healthcare networks to facilitate the differences between theoretical and operational robustness.

To sum up, the next-generation federated intelligence is based on strong aggregation algorithms. With combination of geometric, trust-weighted and secure aggregation, the trifecta of ultra-reliability, scalability and privacy preservation can be ensured in future federated systems with resilient AI functionality in both unreliable and adversarial communication conditions.

References

[1] Pillutla, K., Kakade, S. M., & Harchaoui, Z. (2022). Robust aggregation for federated learning. IEEE Transactions on Signal Processing, 70, 1142-1154. https://doi.org/10.1109/TSP.2022.3153135

[2] Zheng, Y., Lai, S., Liu, Y., Yuan, X., Yi, X., & Wang, C. (2022). Aggregation service for federated learning: An efficient, secure, and more resilient realization. IEEE Transactions on Dependable and Secure Computing, 20(2), 988-1001. https://doi.org/10.1109/TDSC.2022.3146448

[3] Ghosh, A., Hong, J., Yin, D., & Ramchandran, K. (2019). Robust federated learning in a heterogeneous environment. arXiv preprint arXiv:1906.06629. https://doi.org/10.48550/arXiv.1906.06629

[4] Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H., & Raad, A. (2023). Reviewing federated learning aggregation algorithms: Strategies, contributions, limitations, and future perspectives. Electronics, 12(10), 2287. https://doi.org/10.3390/electronics12102287

[5] Tahmasebian, F., Lou, J., & Xiong, L. (2022, October). RobustFed: A truth inference approach for robust federated learning. In Proceedings of the 31st ACM International Conference on Information & Knowledge Management (pp. 1868-1877). https://doi.org/10.1145/3511808.3557439

[6] Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y., & Guizani, M. (2020). Reliable federated learning for mobile networks. IEEE Wireless Communications, 27(2), 72-80. https://doi.org/10.1109/MWC.001.1900119

[7] Sharma, M., & Kaur, P. (2023). Reliable federated learning in a cloud-fog-IoT environment. Journal of Supercomputing, 79(14). https://doi.org/10.1007/s11227-023-05252-w

[8] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics (pp. 1273–1282). PMLR.

[9] Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. IEEE Transactions on Big Data.

[10] Yin, D., Chen, Y., Kannan, R., & Bartlett, P. (2018). Byzantine-robust distributed learning: Towards optimal statistical rates. In International Conference on Machine Learning (pp. 5650-5659). PMLR.

[11] Zhao, L., Jiang, J., Feng, B., Wang, Q., Shen, C., & Li, Q. (2021). SEAR: Secure and efficient aggregation for Byzantine-robust federated learning. IEEE Transactions on Dependable and Secure Computing, 19(5), 3329-3342. https://doi.org/10.1109/TDSC.2021.3093711

[12] Chen, Z., Yi, W., Liu, Y., & Nallanathan, A. (2024). Robust federated learning for unreliable and resource-limited wireless networks. IEEE Transactions on Wireless Communications, 23(8), 9793-9809. https://doi.org/10.1109/TWC.2024.3366393

[13] Wang, R., Yang, L., Tang, T., Yang, B., & Wu, D. (2024). Robust federated learning for heterogeneous clients and unreliable communications. IEEE Transactions on Wireless Communications, 23(10), 13440-13455. https://doi.org/10.1109/TWC.2024.3401395

[14] Khan, N., Nisar, S., Khan, M. A., Rehman, Y. A. U., Noor, F., & Barb, G. (2025). Optimizing federated learning with aggregation strategies: A comprehensive survey. IEEE Open Journal of the Computer Society. https://doi.org/10.1109/OJCS.2025.3590102

[15] Esteves, L., Portugal, D., Peixoto, P., & Falcao, G. (2023). Towards mobile federated learning with unreliable participants and selective aggregation. Applied Sciences, 13(5), 3135. https://doi.org/10.3390/app13053135

[16] Li, Z., Zhou, Y., Wu, D., Tang, T., & Wang, R. (2022). Fairness-aware federated learning with unreliable links in resource-constrained Internet of Things. IEEE Internet of Things Journal, 9(18), 17359-17371. https://doi.org/10.1109/JIOT.2022.3156046

[17] Salehi, M., & Hossain, E. (2021). Federated learning in unreliable and resource-constrained cellular wireless networks. IEEE Transactions on Communications, 69(8), 5136-5151. https://doi.org/10.1109/TCOMM.2021.3081746

[18] Myakala, P. K., & Agrawal, M. (2025). Fault-tolerant federated learning framework for edge devices in unstable networks. Authorea Preprints. https://doi.org/10.36227/techrxiv.174612128.82578829/v1

[19] Yang, Z., Cheng, C., Li, Z., Wang, R., & Zhang, X. (2025). Reliable federated learning based on delayed gradient aggregation for intelligent connected vehicles. Engineering Applications of Artificial Intelligence, 140, 109719. https://doi.org/10.1016/j.engappai.2024.109719

[20] Ang, F., Chen, L., Zhao, N., Chen, Y., Wang, W., & Yu, F. R. (2020). Robust federated learning with noisy communication. IEEE Transactions on Communications, 68(6), 3452-3464. https://doi.org/10.1109/TCOMM.2020.2979149

[21] Li, C.-J., Huang, P.-H., Ma, Y.-T., Hung, H., & Huang, S.-Y. (2022). Robust aggregation for federated learning by minimum γ-divergence estimation. Entropy, 24(5), 686. https://doi.org/10.3390/e24050686

[22] Pillutla, K., Kakade, S. M., & Harchaoui, Z. (2022). Robust aggregation for federated learning. IEEE Transactions on Signal Processing, 70, 1142–1154. https://doi.org/10.1109/TSP.2022.3153135

[23] Miao, Y., et al. (2022). Privacy-preserving Byzantine-robust federated learning. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2022.3196274

[24] Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine-tolerant gradient descent. NeurIPS. https://doi.org/10.5555/3294771.3294783

[25] Cao, X., Fang, M., Liu, J., & Gong, N. Z. (2021). FLTrust: Byzantine-robust federated learning via trust bootstrapping. NDSS Symposium 2021. https://doi.org/10.14722/ndss.2021.24434

[26] Ma, X., Zhou, Y., Wang, L., & Miao, M. (2022). Privacy-preserving Byzantine-robust federated learning. Computer Standards & Interfaces, article 103561. https://doi.org/10.1016/j.csi.2021.103561

[27] Shejwalkar, V., & Houmansadr, A. (2021). Manipulating the Byzantine: Optimizing model poisoning attacks and defenses in federated learning. NDSS 2021. https://doi.org/10.14722/ndss.2021.24498

[28] Zhu, B., et al. (2023). Byzantine-robust federated learning with optimal statistical guarantees. Proceedings / ML Research (PMLR). https://proceedings.mlr.press/v206/zhu23b.html

[29] Pillutla, K., Kakade, S. M., & Harchaoui, Z. (2019). Robust aggregation for federated learning. https://doi.org/10.1109/TSP.2022.3153135

[30] Yan, G., Wang, H., & Yuan, X. (2024). FedRoLA: Robust federated learning against model poisoning via layer-based aggregation. KDD 2024. https://doi.org/10.1145/3637528.3671906