A Complete Proofs for FedAvg

A.1 Proof of Theorem 1

We prove with a reasoning by induction that:

$$\tilde{\theta}^t - \theta^t = \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) + \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i - \nu_i), \quad (26)$$

with $f(\theta^t) = \frac{M_K}{N}\left[\theta^t - \sum_{j\in J} \frac{M_j}{N-M_K}[\eta_j(\theta^t - \theta_j^*) + \theta_j^*]\right]$, $\epsilon = \sum_{j\in J} \frac{M_j}{N}\eta_j$, $\nu_t = \sum_{j\in J} \frac{M_j}{N-M_K}\rho_j\zeta_{j,t}$ and $\tilde{\nu}_t = \sum_{j\in J} \frac{M_j}{N}\rho_j\tilde{\zeta}_{j,t}$. By definition of θ^{t+1}, $\mathbb{E}[f(\theta^t)] = \frac{M_K}{N}\left[\mathbb{E}[\theta^t] - \mathbb{E}\left[\theta^{t+1}\right]\right]$.

Proof. **Server iteration $t = 1$**

Using the fair clients local model parameters evolution of Section 2.3 and the server aggregation process expressed in equation (10), the global model can be written as

$$\theta^1 = \sum_{j\in J} \frac{M_j}{N - M_K}\left[\eta_j\left(\theta^0 - \theta_j^*\right) + \theta_j^*\right] + \nu_0. \quad (27)$$

Similarly, the global model for federated learning with plain free-riders can be expressed as

$$\tilde{\theta}^1 = \sum_{j\in J} \frac{M_j}{N}\left[\eta_j\left(\theta^0 - \theta_j^*\right) + \theta_j^*\right] + \frac{M_K}{N}\theta^0 + \tilde{\nu}_0. \quad (28)$$

By subtracting equation (27) to equation (28), we obtain:

$$\tilde{\theta}^1 - \theta^1 = -\frac{M_K}{N}\sum_{j\in J} \frac{M_j}{N - M_K}\left[\eta_j\left(\theta^0 - \theta_j^*\right) + \theta_j^*\right] + \frac{M_K}{N}\theta^0 + \tilde{\nu}_0 - \nu_0 \quad (29)$$

Hence, $\tilde{\theta}_1 - \theta_1$ follows the formalization.

From t to $t+1$

We suppose the property true at a server iteration t. Hence, we get:

$$\tilde{\theta}^t - \theta^t = \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) + \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i - \nu_i), \quad (30)$$

With the same reasoning as for $t = 1$, we get:

$$\theta^{t+1} = \sum_{j\in J} \frac{M_j}{N - M_K}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] + \nu_t \quad (31)$$

and

$$\tilde{\theta}^{t+1} = \sum_{j\in J} \frac{M_j}{N}\left[\eta_j\left(\tilde{\theta}^t - \theta_j^*\right) + \theta_j^*\right] + \frac{M_K}{N}\tilde{\theta}^t + \tilde{\nu}_t \quad (32)$$

By using equation (30) for equation (32), we get:

$$\begin{aligned}\tilde{\theta}^{t+1} = &\sum_{j\in J} \frac{M_j}{N}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] \\ &+ \epsilon\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) \\ &+ \epsilon\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i - \nu_i) \\ &+ \frac{M_K}{N}\theta^t \\ &+ \frac{M_K}{N}\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) \\ &+ \frac{M_K}{N}\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i - \nu_i) \\ &+ \tilde{\nu}_t \end{aligned} \quad (33)$$

which can be rewritten as:

$$\begin{aligned}\tilde{\theta}^{t+1} = &\sum_{j\in J} \frac{M_j}{N}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] \\ &+ [\epsilon + \frac{M_K}{N}]\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) \\ &+ [\epsilon + \frac{M_K}{N}]\sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i - \nu_i) \\ &+ \frac{M_K}{N}\theta^t + \tilde{\nu}_t, \end{aligned} \quad (34)$$

leading to

$$\begin{aligned}\tilde{\theta}^{t+1} = &\sum_{j\in J} \frac{M_j}{N}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] \\ &+ \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i} f(\theta^i) \\ &+ \sum_{i=0}^{t-1} \left(\epsilon + \frac{M_K}{N}\right)^{t-i} (\tilde{\nu}_i - \nu_i) \\ &+ \frac{M_K}{N}\theta^t + \tilde{\nu}_t \end{aligned} \quad (35)$$

By subtracting equation (35) to equation (31), we obtain:

$$\begin{aligned}\tilde{\theta}^{t+1} - \theta^{t+1} = &-\frac{M_K}{N}\sum_{j\in J}\frac{M_j}{N-M_K}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] \\ &+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i} f(\theta^i) \\ &+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i}(\tilde{\nu}_i - \nu_i) \\ &+ \frac{M_K}{N}\theta^t + \tilde{\nu}_t - \nu_t \end{aligned} \tag{36}$$

Given that $-\frac{M_K}{N}\sum_{j\in J}\frac{M_j}{N-M_K}\left[\eta_j\left(\theta^t - \theta_j^*\right) + \theta_j^*\right] + \frac{M_K}{N}\theta^t = f(\theta^t)$, we get:

$$\begin{aligned}\tilde{\theta}^{t+1} - \theta^{t+1} = &\sum_{i=0}^{t}\left(\epsilon + \frac{M_K}{N}\right)^{t-i} f(\theta^i) \\ &+ \sum_{i=0}^{t}\left(\epsilon + \frac{M_K}{N}\right)^{t-i}(\tilde{\nu}_i - \nu_i). \end{aligned} \tag{37}$$

□

A.2 Proof of Theorem 2

Proof. **Expected Value**

Let us first have a look at the expected value. By definition, a sum of Gaussian distributions with 0 mean, $\mathbb{E}\left[\nu_i\right] = 0$ and $\mathbb{E}\left[\tilde{\nu}_i\right] = 0$. We also notice that $\mathbb{E}\left[f(\theta^t)\right] = \frac{M_K}{N}\left[\mathbb{E}\left[\theta^t\right] - \mathbb{E}\left[\theta^{t+1}\right]\right]$. Hence, we obtain

$$\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = \frac{M_K}{N}\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{n-i-1}\mathbb{E}\left[\theta^t - \theta^{t+1}\right]. \tag{38}$$

We consider that federated learning is converging, hence $|\,\mathbb{E}\left[\theta^t\right] - \mathbb{E}\left[\theta^{t+1}\right]\,| \xrightarrow{t\to+\infty} 0$, and for any positive α, there exists N_0 such that $|\,\mathbb{E}\left[\theta^t - \theta^{t+1}\right]\,| < \alpha$. Since $\eta_j \in]0,1[$, we have $\epsilon \in]0, \frac{N-M_K}{N}[$ and $\epsilon + \frac{M_K}{N} \in]0,1[$. Thus, we can rewrite equation (38) as

$$\begin{aligned}|\,\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right]\,| \le &\sum_{i=0}^{N_0-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}|\,\mathbb{E}\left[\theta^t\right] - \mathbb{E}\left[\theta^{t+1}\right]\,| \\ &+ \sum_{i=N_0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\alpha. \end{aligned} \tag{39}$$

We define by $R_\alpha = \max_{i\in[1,N_0]}|\,\mathbb{E}\left[\theta^t\right] - \mathbb{E}\left[\theta^{t+1}\right]\,|$, and get:

$$\begin{aligned}|\,\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right]\,| \le &\underbrace{\sum_{i=0}^{N_0-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}}_{A} R_\alpha \\ &+ \underbrace{\sum_{i=N_0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}}_{B}\alpha. \end{aligned} \tag{40}$$

- **Expressing A.**

$$A = \sum_{i=0}^{N_0-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} \tag{41}$$

$$= \left(\epsilon + \frac{M_K}{N}\right)^{t-1}\frac{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-N_0}}{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-1}} \tag{42}$$

$$\xrightarrow{t\to+\infty} 0 \tag{43}$$

- **Expressing B.**

$$B = \sum_{i=N_0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} \tag{44}$$

$$= \left(\epsilon + \frac{M_K}{N}\right)^{t-N_0-1}\frac{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-(t-N_0)}}{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-1}} \tag{45}$$

$$= \frac{1 - \left(\epsilon + \frac{M_K}{N}\right)^{t-N_0}}{1 - \left(\epsilon + \frac{M_K}{N}\right)} \tag{46}$$

$$\xrightarrow{t\to+\infty} \frac{1}{1 - \left(\epsilon + \frac{M_K}{N}\right)} > 0 \tag{47}$$

Using equation (43) and (47) in equation (40), we get:

$$\forall\alpha \lim_{t\to+\infty}|\,\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right]\,| \le B\alpha, \tag{48}$$

which is equivalent to

$$\lim_{t\to+\infty}\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = 0. \tag{49}$$

Variance

The Wiener processes, ν_i and $\tilde{\nu}_i$ are independent from the server models parameters θ^i. Also, each Wiener process is independent with the other Wiener processes. Hence, we get:

$$\begin{aligned}\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] = &\underbrace{\mathrm{Var}\left[\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i)\right]}_{E} \\ &+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{2(t-i-1)}\underbrace{\mathrm{Var}\left[\tilde{\nu}_i - \nu_i\right]}_{F}, \end{aligned} \tag{50}$$

Expressing E. Before getting a simpler expression for E, we need to consider $\text{Cov}\left[f(\theta^l), f(\theta^m)\right]$. To do so, we first consider $f(\theta^t) - \mathbb{E}\left[f(\theta^t)\right]$.

$$f(\theta^t) - \mathbb{E}\left[f(\theta^t)\right] = \underbrace{\frac{M_K}{N}\left[1 - \sum_{j\in J}\frac{M_j}{N-M_K}\eta_j\right]}_{G}[\theta^t - \mathbb{E}\left[\theta^t\right]], \quad (51)$$

We can prove with a reasoning by induction that $\theta^t - \mathbb{E}\left[\theta^t\right] = \sum_{i=0}^{n-1}\left(\sum_{j\in J}\frac{M_j}{N-M_K}\eta_j\right)^{t-i-1}\nu_i = \sum_{k=0}^{n-1}\epsilon^{t-i-1}\nu_i$. All the ν_i are independent across each others and have 0 mean, hence:

$$\text{Cov}\left[f(\theta_l), f(\theta_m)\right] = G^2\sum_{i=0}^{\min\{l-1,m-1\}}\epsilon^{l+m-2i-2}\,\mathbb{E}\left[\nu_i^2\right] \quad (52)$$

Considering that $\mathbb{E}\left[\nu_i^2\right] = \text{Var}\left[\nu_i\right] = \sum_{j\in J}\left(\frac{M_j}{N-M_K}\rho_j\right)^2$, we get:

$$\text{Cov}\left[f(\theta^l), f(\theta^m)\right] = G^2\sum_{j\in J}\left(\frac{M_j}{N-M_K}\rho_j\right)^2\sum_{i=0}^{2\min\{l-1,m-1\}}\epsilon^{t-i-1} \quad (53)$$

We define $G' = G^2\sum_{j\in J}\left(\frac{M_j}{N-M_K}\rho_j\right)^2$. Given that $\epsilon \in]0,1[$, we get the following upper bound on E:

$$\text{Cov}\left[f(\theta^l), f(\theta^m)\right] \leq G'\min\{l,m\} \quad (54)$$

By denoting $H = \epsilon + \frac{M_K}{N}$, we can rewrite E as:

$$E = \sum_{l=0}^{t-1}\sum_{m=0}^{t-1}H^{2(t-1)-l-m}\,\text{Cov}\left[f_l(\theta^l), f(\theta^m)\right] \quad (55)$$

$$\leq \sum_{l=0}^{t-1}\sum_{m=0}^{t-1}H^{2(t-1)-l-m}G'\min\{l,m\} \quad (56)$$

Considering that $\min\{l,m\} \leq l$, we get:

$$E \leq G'\sum_{l=0}^{t-1}\sum_{m=0}^{t-1}H^{2(t-1)-l-m}l \quad (57)$$

$$= G'H^{2(t-1)}\sum_{l=0}^{t-1}H^{-l}l\sum_{m=0}^{t-1}H^{-m} \quad (58)$$

$$= G'H^{2(t-1)}\sum_{l=0}^{t-1}H^{-l}l\frac{1-H^{-n}}{1-H^{-1}} \quad (59)$$

$$= G'H^{2(t-1)}\frac{1-H^{-n}}{1-H^{-1}}\sum_{l=0}^{t-1}H^{-l}l \quad (60)$$

Considering the power series $\sum_{k=0}^{+\infty}nx^n = \frac{x}{(1-x)^2}$, we get that $\sum_{l=0}^{t-1}H^{-l}l = \frac{H^{-1}}{(1-H^{-1})^2}$. Hence, E's upper bound goes to 0. Given that E is non-negative, we get:

$$E \xrightarrow{t\to+\infty} 0 \quad (61)$$

Expressing F. Let us first consider the noise coming from the SGD steps. All the $\tilde{\nu}_i$ are independent with ν_i. Hence, we have

$$F = \text{Var}\left[\tilde{\nu}_i\right] - \text{Var}\left[\nu_i\right] \quad (62)$$

$$= \text{Var}\left[\sum_{j\in J}\frac{M_j}{N}\rho_j\tilde{\zeta}_{j,i} - \sum_{j\in J}\frac{M_j}{N-M_K}\rho_j\zeta_{j,i}\right] \quad (63)$$

$$= [\frac{1}{N^2} + \frac{1}{(N-M_K)^2}]\sum_{j\in J}\left(M_j\rho_j\right)^2 \quad (64)$$

Replacing (64) in equation (50), we can express the variance as

$$\text{Var}\left[\tilde{\theta}^t - \theta^t\right] = E + F\sum_{i=0}^{t-1}H^{2(t-i-1)} \quad (65)$$

$$= E + FH^{2(t-1)}\sum_{i=0}^{t-1}H^{-2i} \quad (66)$$

$$= E + FH^{2(t-1)}\frac{1-H^{-2t}}{1-H^{-2}} \quad (67)$$

$$= E + F\frac{1-H^{2t}}{1-H^2} \quad (68)$$

By replacing F and H with their respective expression, we can conclude that

$$\text{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} \frac{[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}]\sum_{j\in J}\left(M_j\rho_j\right)^2}{1-\left(\epsilon + \frac{M_K}{N}\right)^2} \quad (69)$$

□

Note 1: The asymptotic variance is strictly increasing with the number of data points declared by the free-riders M_K.

While M_j and ρ_j are constants and independent from the number of free-riders and from their respective number of data points, N and ϵ depend on the total number of free-riders' samples M_K. We first rewrite $\epsilon = \frac{1}{N}\alpha$ with $\alpha = \sum_{j\in J}M_j\eta_j$ not depending on M_K and we get:

$$\epsilon + \frac{M_K}{N} = \frac{1}{N}[\alpha + M_K]. \quad (70)$$

By defining $M_J = \sum_{j\in J}M_j$, we get:

$$1 - \left(\epsilon + \frac{M_K}{N}\right)^2 = \frac{1}{N^2}[M_J^2 + 2M_K[M_J - \alpha] - \alpha^2], \quad (71)$$

with $M_J - \alpha > 0$ because $\eta_j \in]0, 1[$.

Also, considering that

$$\frac{1}{N^2} + \frac{1}{(N - M_K)^2} = \frac{1}{N^2}[\frac{M_K^2}{M_J^2} + 2\frac{M_K}{M_J} + 2], \quad (72)$$

we can rewrite

$$\frac{\frac{1}{N^2} + \frac{1}{(N-M_K)^2}}{1 - \left(\epsilon + \frac{M_K}{N}\right)^2} = \frac{\frac{M_K^2}{M_J^2} + 2\frac{M_K}{M_J} + 2}{M_J^2 + 2M_K[M_J - \alpha] - \alpha^2} \quad (73)$$

As the numerator is a polynomial of order 2 in M_K and the denominator is a polynomial of order 1 in M_K, the asymptotic variance is increasing with M_K.

Note 2: When considering that the SGD noise variance is different for federated learning with and without free-riders, we get:

$$F = \frac{1}{N^2}\sum_{j \in J}(M_j \tilde{\rho}_j)^2 + \frac{1}{(N - M_K)^2}\sum_{j \in J}(M_j \rho_j)^2 \quad (74)$$

A.3 Proof of Theorem 3

Proof. **Relation between federated learning with and without free-riders global model**

With a reasoning by induction similar to Proof A.1, we get:

$$\tilde{\theta}^t - \theta^t = \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) \quad (75)$$

$$+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}(\tilde{\nu}_i - \nu_i) \quad (76)$$

$$+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_K}{N}\varphi\epsilon_t, \quad (77)$$

Expected value

ϵ_t is a delta-correlated Gaussian White noise which implies that $\mathbb{E}[\epsilon_t] = 0$. Following the same reasoning steps as in Proof A.2, we get:

$$\lim_{t \to +\infty} \mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = 0. \quad (78)$$

Variance

All the ϵ_t are independent Gaussian white noises implying $\mathrm{Var}[\epsilon_t] = 1$. Following the same reasoning steps as in Proof A.2, we get:

$$\mathrm{Var}\left[\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_K}{N}\varphi\epsilon_t\right]$$

$$= \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{2(t-i-1)}\frac{M_K^2}{N^2}\varphi^2 \quad (79)$$

$$= \left(\epsilon + \frac{M_K}{N}\right)^{2(t-1)}\frac{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-2t}}{1 - \left(\epsilon + \frac{M_K}{N}\right)^{-2}}\frac{M_K^2}{N^2}\varphi^2 \quad (80)$$

$$= \frac{1 - \left(\epsilon + \frac{M_K}{N}\right)^{2t}}{1 - \left(\epsilon + \frac{M_K}{N}\right)^2}\frac{M_K^2}{N^2}\varphi^2 \quad (81)$$

$$\xrightarrow{t \to +\infty} \frac{1}{1 - \left(\epsilon + \frac{M_K}{N}\right)^2}\frac{M_K^2}{N^2}\varphi^2 \quad (82)$$

As for equation (50), all the ϵ_t are independent from ν_t, from $\tilde{\nu}_t$, and from the global model parameters θ^t. Hence, for one disguised free-rider we get the following asymptotic variance:

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t \to +\infty} \frac{[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}]\sum_{j \in J}(M_j \rho_j)^2}{1 - \left(\epsilon + \frac{M_K}{N}\right)^2} + \frac{1}{1 - \left(\epsilon + \frac{M_K}{N}\right)^2}\frac{M_K^2}{N^2}\varphi^2. \quad (83)$$

□

A.4 Proof of Corollary 1

Proof. **Relation between federated learning with and without free-riders global model**

With a reasoning by induction similar to Proof A.1, we get:

$$\tilde{\theta}^t - \theta^t = \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1} f(\theta^i) \quad (84)$$

$$+ \sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}(\tilde{\nu}_i - \nu_i) \quad (85)$$

$$+ \sum_{k \in K}\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_k}{N}\varphi_k\epsilon_{k,t}, \quad (86)$$

Expected value

$\epsilon_{k,t}$ are delta-correlated Gaussian White noises which implies that $\mathbb{E}[\epsilon_{k,t}] = 0$. Following the same reasoning steps as in Proof A.2, we get:

$$\lim_{t \to +\infty} \mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = 0. \quad (87)$$

Variance

All the $\epsilon_{k,t}$ are independent Gaussian white noises over server iterations t and free-riders indices k implying $\mathrm{Var}\left[\epsilon_t\right] = 1$. Following the same reasoning steps as in Proof A.2, we get:

$$\mathrm{Var}\left[\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_k}{N}\varphi_k\epsilon_{k,t}\right] \xrightarrow{t\to+\infty} \frac{1}{1-\left(\epsilon+\frac{M_K}{N}\right)^2}\frac{M_k^2}{N^2}\varphi_k^2 \tag{88}$$

Like for equation (50), all the $\epsilon_{k,t}$ are independent from ν_t, $\tilde{\nu}_t$ and the global model parameters θ^t. Hence, for multiple disguised free-rider we get the following asymptotic variance:

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} \frac{\left[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}\right]\sum_{j\in J}\left(M_j\rho_j\right)^2}{1-\left(\epsilon+\frac{M_K}{N}\right)^2} + \frac{1}{1-\left(\epsilon+\frac{M_K}{N}\right)^2}\sum_{k\in K}\frac{M_k^2}{N^2}\varphi_k^2. \tag{89}$$

□

A.5 Proof of Corollary 2

Proof. **Relation between federated learning with and without free-riders global model**

The relation remains the same for Theorem 2, Theorem 3, and Corollary 1 by replacing η_j with $\eta_j(t) = \sum j \in J\frac{M_j}{N}\rho_j(t)$ and φ_k by $\varphi_k(t)$ for disguised free-riding.

Expected value

With ρ_j^t and $\varphi(t)$ the properties for $\tilde{\nu}_t$, ν_t, ϵ_t and $\epsilon_{k,t}$ remain identical. Hence, they still are delta-correlated Gaussian White noises implying that $\mathbb{E}\left[\tilde{\nu}_t\right] = \mathbb{E}\left[\nu_t\right] = \mathbb{E}\left[\epsilon_t\right] = \mathbb{E}\left[\epsilon_{k,t}\right] = 0$. Hence, for Theorem 2, Theorem 3, and Corollary 1, we get:

$$\lim_{t\to+\infty}\mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = 0. \tag{90}$$

Variance

Variance asymptotic behaviour proven in Proof A.2, A.3, and A.4 can be reduced to the one in Proof A.2. Hence, F, equation (64), need to be reexpressed to take into account $\rho_j(t)$. All the $\tilde{\nu}_i$ are still independent with ν_i. Hence, we have:

$$F = \mathrm{Var}\left[\tilde{\nu}_i(t) - \nu_i(t)\right] \tag{91}$$

$$= \mathrm{Var}\left[\sum_{j\in J}\frac{M_j}{N}\rho_j^t\tilde{\zeta}_{j,i} - \sum_{j\in J}\frac{M_j}{N-M_K}\rho_j^t\zeta_{j,i}\right] \tag{92}$$

Considering that $\rho_j^t \xrightarrow{t\to+\infty} 0$, we get:

$$F \xrightarrow{t\to+\infty} 0 \tag{93}$$

Using the same reasoning as the one used for the expected value convergence in Proof A.2, we get that the SGD noise contribution linked to F goes to 0 at infinity.

For the disguised free-riders, $\epsilon_{k,t}$ are still independent Gaussian white noises implying $\mathrm{Var}\left[\epsilon_{k,t}\right] = 1$. Hence, following a reasoning similar to the on in Proof A.2, we get:

$$\mathrm{Var}\left[\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_K}{N}\varphi_k(t)\epsilon_{k,t}\right] = \sum_{i=0}^{t-1}\left(\epsilon+\frac{M_K}{N}\right)^{2(t-i-1)}\frac{M_K^2}{N^2}\varphi_k^2(t) \tag{94}$$

Considering that $\varphi_k(t) \xrightarrow{t\to+\infty} 0$, by using the same reasoning as for the proof of the expected value for free-riders, Section XX, we get:

$$\mathrm{Var}\left[\sum_{i=0}^{t-1}\left(\epsilon + \frac{M_K}{N}\right)^{t-i-1}\frac{M_K}{N}\varphi_k(t)\epsilon_{k,t}\right] \xrightarrow{t\to+\infty} 0 \tag{95}$$

Hence, we can conclude that

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} 0. \tag{96}$$

□

B Complete Proofs for FedProx

FedProx is a generalization of FedAvg. As such, we use the proof done for FedAvg to prove convergence of free-riders attack using FedProx as an optimization solver. The L2 norm monitored by μ changes the gradient as $g_j(\theta_j) \simeq r_j[\theta_j - \theta_j^*] + \mu[\theta_j - \theta^t]$.

Using equation (7), we then get:

$$\mathrm{d}\theta_j = -\lambda\left[r_j[\theta_j - \theta_j^*] + \mu[\theta_j - \theta^t]\right] + \frac{\lambda}{\sqrt{S}}\sigma_j(\theta_j)\mathrm{d}W_j, \tag{97}$$

leading to

$$\theta_j(u) = e^{-\lambda[r_j+\mu]u}\theta_j(0) + \frac{r_j\theta_j^* + \mu\theta^t}{r_j+\mu}[1 - e^{-\lambda(r_j+\mu)u}] + \frac{\lambda}{\sqrt{S}}\int_{x=0}^{u}e^{-\lambda(r_j+\mu)(u-x)}\sigma_j(\theta_j)\mathrm{d}W_x. \tag{98}$$

considering that $\theta_j(0) = \theta^t$, $\theta_j(\frac{EM_j}{S}) = \theta_j^{t+1}$, and

$\sigma_j(\theta_j) = \sigma_j^t$, we get:

$$\theta_j^{t+1} = \gamma_j \theta^t + \frac{r_j \theta_j^* + \mu \theta^t}{r_j + \mu}[1 - \gamma_j] \quad (99)$$

$$+ \frac{\lambda}{\sqrt{S}} \int_{x=0}^{\frac{EM_j}{S}} e^{-\lambda(r_j+\mu)(\frac{EM_j}{S} - x)} \sigma_j^t \mathrm{d}W_x, \quad (100)$$

where $\gamma_j = e^{-\lambda[r_j+\mu]\frac{EM_j}{S}}$. We can reformulate this as

$$\theta_j^{t+1} = [\gamma_j + \mu \frac{1-\gamma_j}{r_j+\mu}]\theta^t + \frac{r_j}{r_j+\mu}[1-\gamma_j]\theta_j^* \quad (101)$$

$$+ \frac{\lambda}{\sqrt{S}} \int_{x=0}^{\frac{EM_j}{S}} e^{-\lambda(r_j+\mu)(\frac{EM_j}{S} - x)} \sigma_j^t \mathrm{d}W_x, \quad (102)$$

The SGD noise variance between two server iterations for FedProx is:

$$\mathrm{Var}\left[\theta_j^{t+1} | \theta^t\right] = \underbrace{\frac{\lambda}{S} {\sigma_j^t}^2 \frac{1}{2(r_j+\mu)} \left[1 - e^{-2\lambda(r_j+\mu)\frac{EM_j}{S}}\right]}_{{\rho_j^t}^2}, \quad (103)$$

We also define $\eta_j' = \gamma_j + \mu \frac{1-\gamma_j}{r_j+\mu}$ and $\delta_j = \frac{r_j}{r_j+\mu}[1-\gamma_j]$. For FedAvg, $\mu = 0$, we get $\eta_j' = \eta_j$ and $\delta_j = 1 - \eta_j$. By property of the exponential, $\gamma_j \in]0,1[$. As r_j and μ are non negative, then $\eta_j' \in]0,1[$ like η_j for FedAvg.

Theorem 1 for FedProx

We consider ${\rho_j'}^2 = \frac{\lambda}{S} {\sigma_j}^2 \frac{1}{2(r_j+\mu)} \left[1 - e^{-2\lambda(r_j+\mu)\frac{EM_j}{S}}\right]$

Using the same reasoning by induction as in Proof A.1, we get:

$$\tilde{\theta}^t - \theta^t = \sum_{i=0}^{t-1} \left(\epsilon' + \frac{M_K}{N}\right)^{t-i-1} g(\theta^i)$$

$$+ \sum_{i=0}^{t-1} \left(\epsilon' + \frac{M_K}{N}\right)^{t-i-1} (\tilde{\nu}_i' - \nu_i'), \quad (104)$$

with $g(\theta^t) = \frac{M_K}{N}\left[\theta^t - \sum_{j\in J} \frac{M_j}{N-M_K}[\eta_j'\theta^t + \delta_j \theta_j^*]\right]$, $\epsilon' = \sum_{j\in J} \frac{M_j}{N} \eta_j'$, $\nu_t' = \sum_{j\in J} \frac{M_j}{N-M_K} \rho_j' \zeta_{j,t}$ and $\tilde{\nu}_t' = \sum_{j\in J} \frac{M_j}{N} \rho_j' \tilde{\zeta}_{j,t}$.

Theorem 2 for FedProx

Like for FedAvg, we make the assumption that federated learning without free-riders using FedProx converge. In addition, $\tilde{\nu}_t'$ and ν_t' are also independent delta-correlated Gaussian white noises. Following the same proof as in Proof A.2, we thus get:

$$\lim_{t\to+\infty} \mathbb{E}\left[\tilde{\theta}^t - \theta^t\right] = 0. \quad (105)$$

and

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} \frac{[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}] \sum_{j\in J} \left(M_j \rho_j'\right)^2}{1 - \left(\epsilon' + \frac{M_K}{N}\right)^2} \quad (106)$$

The asymptotic variance still strictly increases with M_K.

Note: We introduce $x = \lambda(r_j + \mu)\frac{EM_j}{S}$. By taking the partial derivative of ρ_j' with respect to μ, we get:

$$\frac{\delta \rho_j'}{\delta \mu} = \frac{\lambda}{2S} \sigma_j^2 \frac{1}{(r_j+\mu)^2}[-1 + (1+2x)e^{-2x}], \quad (107)$$

which is strictly negative for a positive μ considering that all the other constants are positive. Hence, the SGD noise variance ρ_j' is inversely proportional with the regularization factor μ.

Similarly, for ϵ', by considering that η_j' can be rewritten as $\eta_j' = \gamma_j \frac{r_j}{r_j+\mu} + \frac{\mu}{r_j+\mu}$, the partial derivative of η_j' with respect to μ can be expressed as:

$$\frac{\delta \eta_j'}{\delta \mu} = \frac{r_j}{(r_j+\mu)^2}[1 - (1-x)e^{-x}], \quad (108)$$

which is strictly positive. Hence η_j' is strictly increasing with the regularization μ and so is ϵ'.

Considering the behaviours of ϵ' and ρ_j' with respect to the regularization term μ, the more regularization is asked by the server and the smaller the asymptotic variance is, leading to more accurate free-riding attacks.

Theorem 3 for FedProx

The free-riders mimic the behaviour of the fair clients. Hence, we get:

$${\varphi_k'}^2 = \frac{\lambda}{S} {\sigma_k}^2 \frac{1}{2(r_j+\mu)} \left[1 - e^{-2\lambda(r_k+\mu)\frac{EM_j}{S}}\right] \quad (109)$$

leading to

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} \frac{[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}] \sum_{j\in J} \left(M_j \rho_j'\right)^2}{1 - \left(\epsilon' + \frac{M_K}{N}\right)^2}$$

$$+ \frac{1}{1 - \left(\epsilon' + \frac{M_K}{N}\right)^2} \frac{M_K^2}{N^2} \varphi'^2. \quad (110)$$

For disguised free-riders, the variance is also inversely proportional to the regularization parameter μ.

Corollary 1 for FedProx

Similarly, for many free-riders, we get:

$$\mathrm{Var}\left[\tilde{\theta}^t - \theta^t\right] \xrightarrow{t\to+\infty} \frac{[\frac{1}{N^2} + \frac{1}{(N-M_K)^2}] \sum_{j\in J} \left(M_j \rho_j'\right)^2}{1 - \left(\epsilon' + \frac{M_K}{N}\right)^2}$$

$$+ \frac{1}{1 - \left(\epsilon' + \frac{M_K}{N}\right)^2} \frac{M_K^2}{N^2} \sum_{k\in K} \varphi_k'^2. \quad (111)$$

C Additional experimental results

C.1 Accuracy Performances

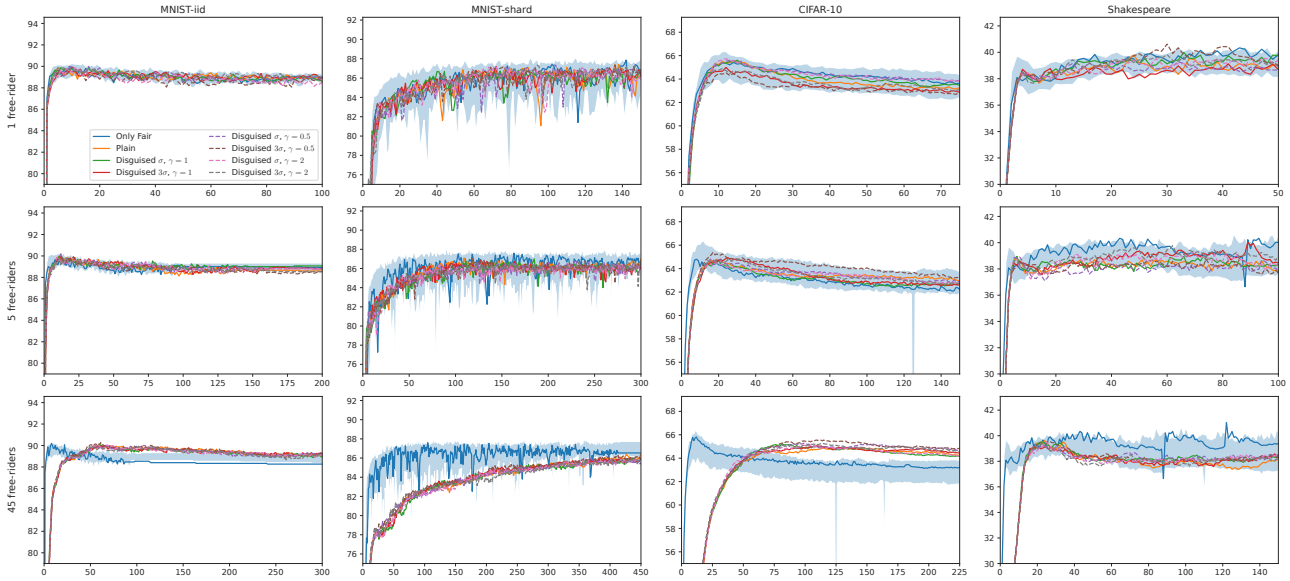

Figure 3: Accuracy performances for FedAvg and 20 epochs in the different experimental scenarios.

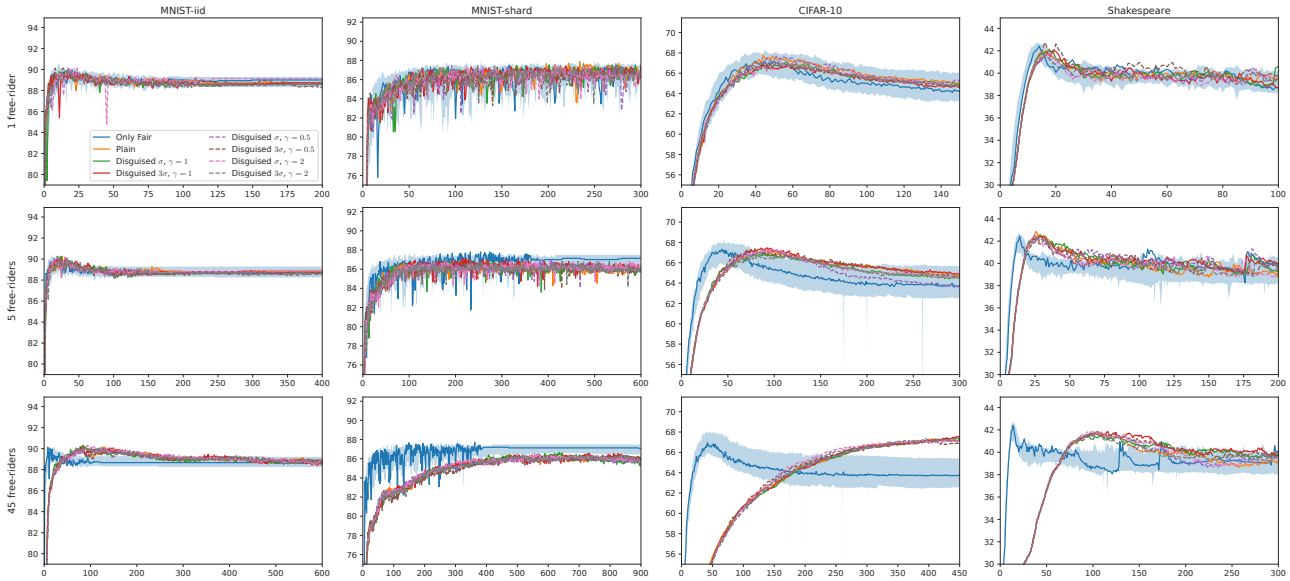

Figure 4: Accuracy performances for FedAvg and 5 epochs in the different experimental scenarios.

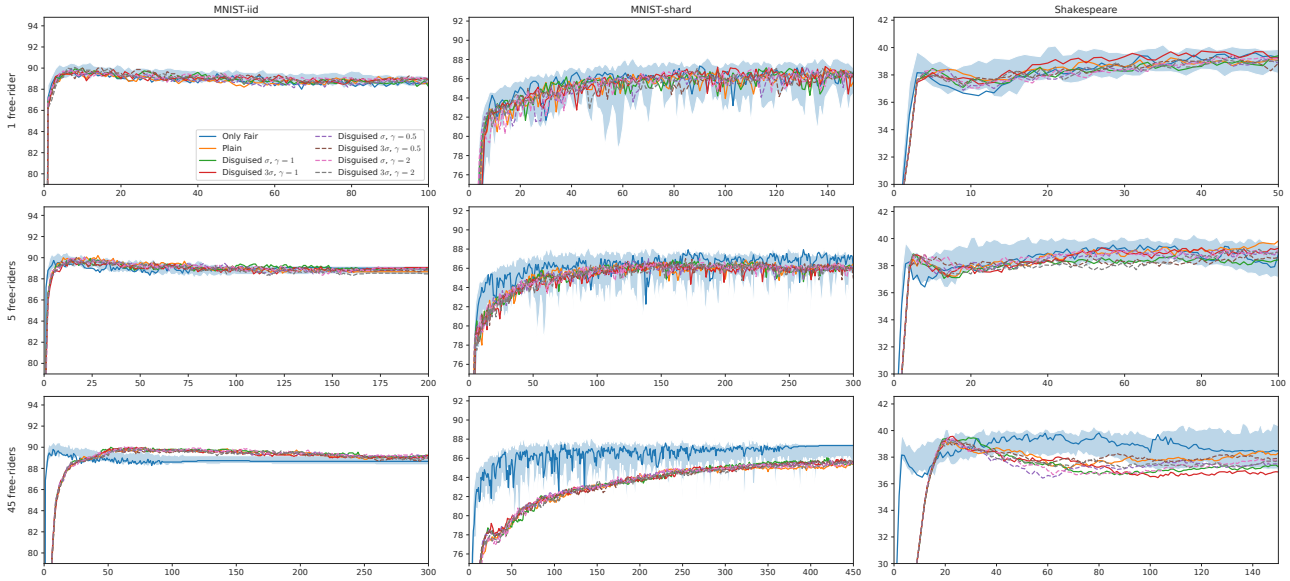

Figure 5: Accuracy performances for FedProx and 20 epochs in the different experimental scenarios.

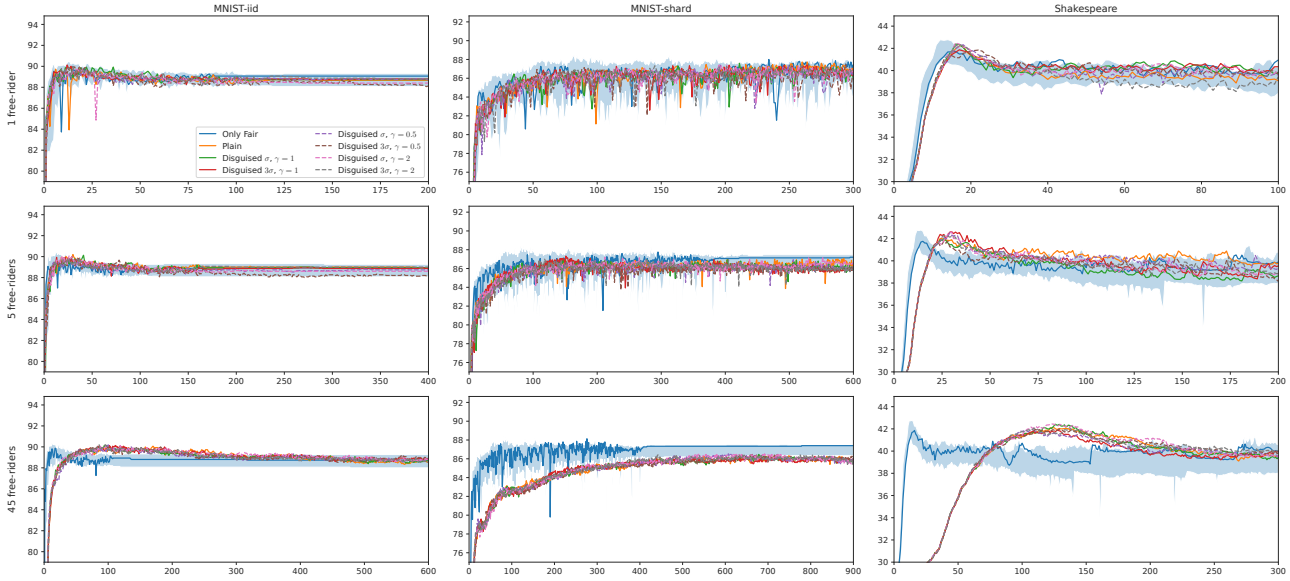

Figure 6: Accuracy performances for FedProx and 5 epochs in the different experimental scenarios.

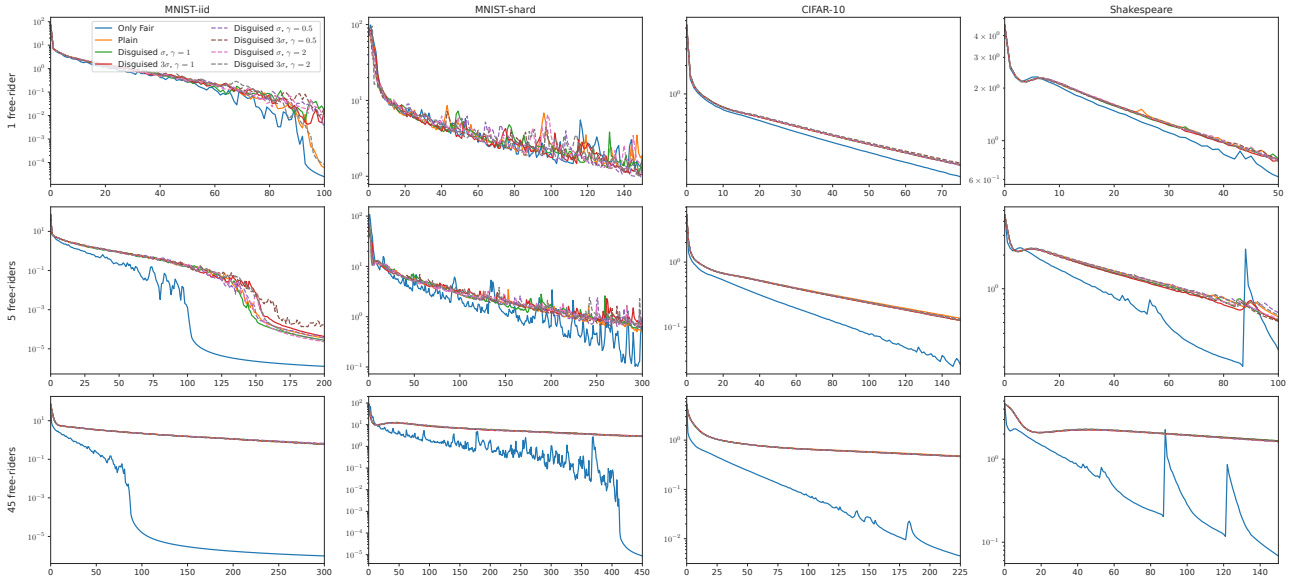

Figure 7: Loss performances for FedAvg and 20 epochs in the different experimental scenarios.

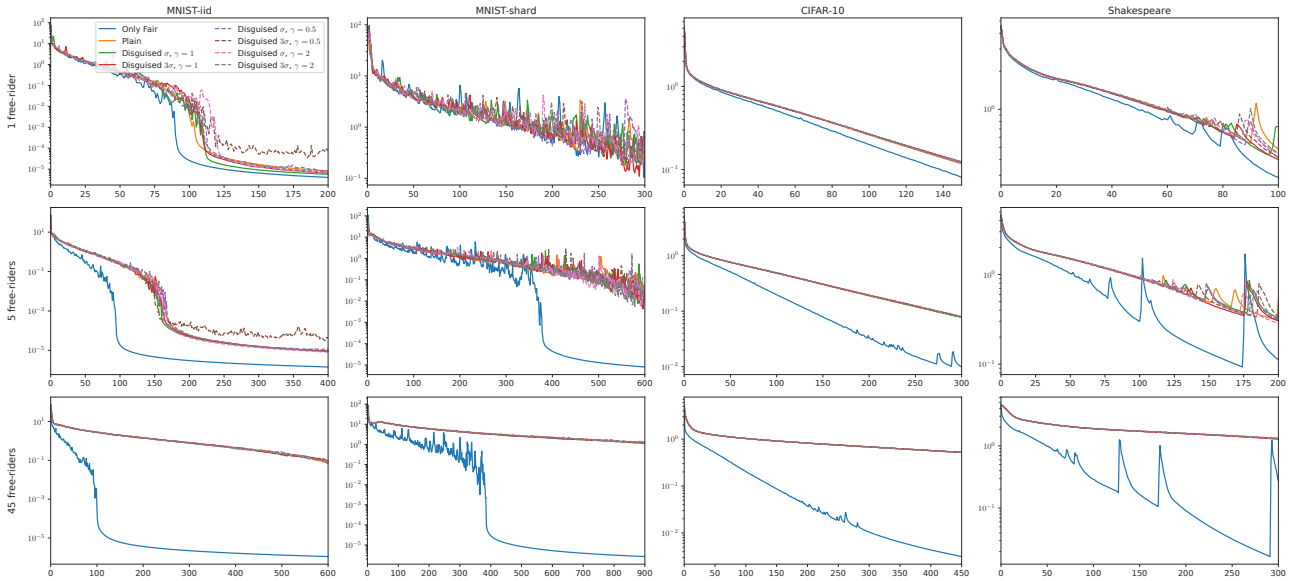

Figure 8: Loss performances for FedAvg and 5 epochs in the different experimental scenarios.

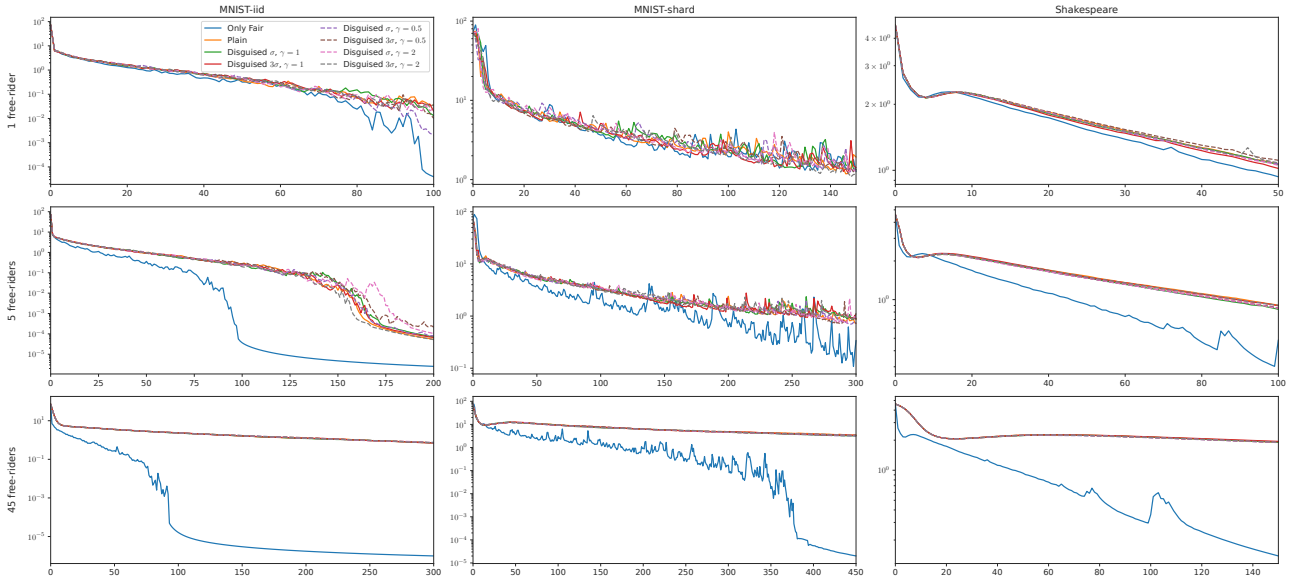

Figure 9: Loss performances for FedProx and 20 epochs in the different experimental scenarios.

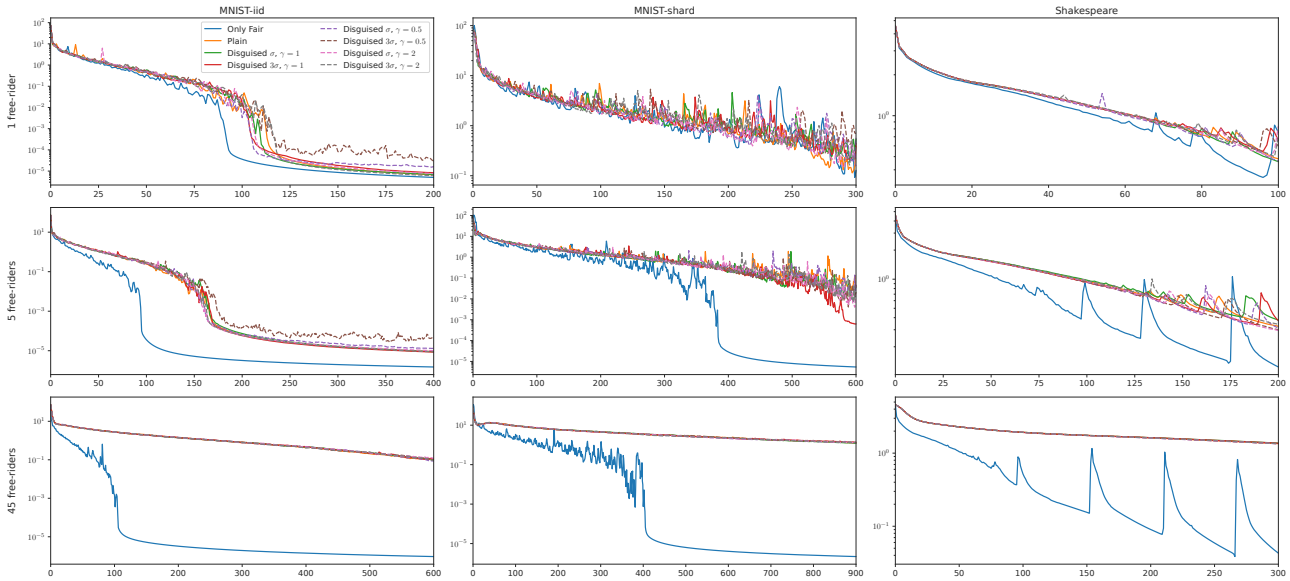

Figure 10: Loss performances for FedProx and 5 epochs in the different experimental scenarios.