Particle Anti-Particle Method for Feature Privacy Protection in Weighted Aggregation in Federated Learning

Varun Kukreti

September 2024

1 Abstract

The protocol proposed in original paper ensures that each client or insurer encrypts their model parameters before sending to the central server and the central server calculates the arithmetic average of the model parameters WITHOUT decrypting the data. This ensures that the privacy of the features of an insurer is maintained to a good extent. However, here we assumed that all the insurers have equal contribution and thus have the same amount of weightage provided in the aggregation stage.

We now propose a new approach which incorporates details from the previous approach can be easily extended to the cases where the insurers have different amounts of weightage or importance w_i provided to them which occurs more commonly in real-life senarios. The empirical graph in such cases has an edge weight assigned to the edge between central server and respective insurer indicating the amount of importance given to a particular insurer during the aggregation. This approach has the advantages of easy implementation and is very robust and mathematically efficient.

2 Background

If all the clients have same amount of contribution to the aggregation stage then the central server C calculates the aggregation of parameters as:

$$\tilde{\beta} = \frac{1}{n} \sum_{i=0}^{n} \tilde{\beta}_i$$

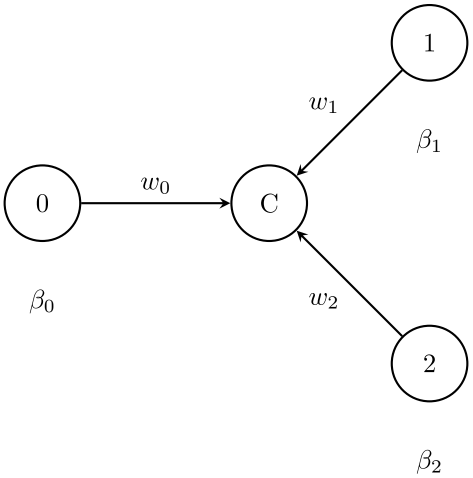
However, if each of the client has different importance then the central server C now calculates weighted average aggregation $\tilde{\beta_w}$ instead of the average aggregation as shown below:

$$\tilde{\beta_w} = \frac{1}{W}\sum_{i=0}^{n} w_i\tilde{\beta}_i$$

where

$$W = \sum_{i=0}^{n} w_i$$

The empirical graph in such cases has an edge weight on the edges between the client and server. A typical such arrangemet with 3 clients is shown here:



3 Initial Setup

Our work is based on the concept of exchange of particle and anti-particle between the clients. In this modified approach the clients do not share the parameters that carry sensitive information. We however make them share information regarding the importance or weight attached to each client along with the particle and anti particle that carries it.

So now for each particle exchanged we take two more things - 1. weight of its source and 2. weight of its destination

4 Mathematical approach

The weighted aggregation at central server is given as :

$$\tilde{\beta_w} = \frac{1}{W}\sum_{i=0}^{n} w_i\tilde{\beta}_i$$

where

$$W = \sum_{i=0}^{n} w_i$$

Let us say we have k number of clients and client i has edge weight w_i and parameter β_i. The client will send a particle to all other clients and will receive anti-particles from all other clients as well. Let θ_i denote a particle and γ_i denote the anti-particle send. So the overall information send to the server by client i is given as

$$\beta_i + \sum_{j=0, j!=i}^{n} (w_j\theta_j - w_j\gamma_j)$$

Now each of client i sends this information to the server. The server then calculates the overall aggregation for client i by multiplying with edge weight w_i as

$$w_i(\beta_i + \sum_{j=0, j!=i}^{n} (w_j\theta_j - w_j\gamma_j))$$

So we obtain the following

$$\tilde{\beta_w} = \frac{1}{W}(\sum_{i=0}^{n} w_i(\beta_i + \sum_{j=0, j!=i}^{n} (w_j\theta_j - w_j\gamma_j)))$$

$$\tilde{\beta_w} = \frac{1}{W}(\sum_{i=0}^{n} w_i\beta_i + \sum_{i=0}^{n} \sum_{j=0, j!=i}^{n} w_i(w_j\theta_j - w_j\gamma_j)))$$

$$\tilde{\beta_w} = \frac{1}{W}(\sum_{i=0}^{n} w_i\beta_i + \sum_{i=0}^{n} \sum_{j=0, j!=i}^{n} (w_iw_j\theta_j - w_iw_j\gamma_j)))$$

The particle for one is anti particle for other. Thus the overall aggregation sum will cancel the weighted particle-antiparticle summation terms i.e.,

$$w_iw_j\theta_j = w_jw_i\gamma_j$$

Thus the second summation cancels out. So we obtain the overall result as:

$$\tilde{\beta_w} = \frac{1}{W}\sum_{i=0}^{n} w_i\beta_i$$

where

$$W = \sum_{i=0}^{n} w_i$$

Thus we proved using simple mathematics as well that such a novel approach works well.

5 Example

Consider 3 clients/insurer $i = 0, 1, 2$, with model parameters β_i as follows. Also now we attach importance to the each client as well:

Insurer i	Model Parameter β_i	Importance
0	1.6	33
1	0.9	21
2	1.4	85

The required weighted average parameter value is therefore

$$\frac{1.6 \times 33 + 0.9 \times 21 + 1.4 \times 85}{33 + 21 + 85} = 1.372.$$

Lets again use the same concept of particle physics with little modifications. We consider each insurer securely sends an encrypted arbitrary random number multiplied with its edge weight, which we will call a "Particle," to each insurer in the modeling exercise. For example:

- Insurer 0 sends insurer 1 the "Particle"

  $$2.3 \times 33 = 75.9$$

  , and insurer 2 the "Particle"

  $$17 \times 33 = 561$$

  .

- Insurer 1 sends insurer 0 the "Particle"

  $$99 \times 21 = 2079$$

  , and insurer 2 the "Particle"

  $$0.1 \times 21 = 2.1$$

  .

- Insurer 2 sends insurer 0 the "Particle"

  $$5 \times 85 = 425$$

  ,, and insurer 1 the "Particle"

  $$20 \times 85 = 1700$$

  .

Thus now we send the "Particle" and "Anti-Particle" by multiplying it with appropriate edge-weight as well. Thus we have:

Insurer i	Parameter β_i	Sent "Particles"	Received "Particles" / "Antiparticles"
0	1.6	[75.9x21, 561x85]	[2079x21, 425x85]
1	0.9	[2079x33, 2.1x85]	[75.9x33, 1700x85]
2	1.4	[425x33, 1700x21]	[561x33, 2.1x21]

We the perform the weighted aggregation and get the same result as above

6 Proposed Work

We propose to examine the working of this method by training standard model in an FL environment - with and without using the Particle Anti-Particle Method on Benchmark Datasets like MNIST to show that there is no considerable difference in the test results obtained in these two settings.

6.1 Workflow:

1. Make solid mathematical foundations
2. Test it on some model for multiple number of clients and atleast for 3 standard datasets - (MNIST, CIFAR10, FEMNIST) in 2 senarios FL without and WITH this concept. (Require resourses)
3. Publish :)