ECML PKDD 2024

fluke: federated learning utility framework for experimentation and research

Mirko Polato, PhD Department of Computer Science, University of Turin, Italy mirko.polato@unito.it

2nd Workshop on Advancement in Federated Learning @ ECML PKDD 2024



DI TORINO





Yet another FL framework? Not really!











through the implementation

to testing

Yet another FL framework? Not really!



from the idea

through the implementation





fluke

to testing



Main features of fluke

Designed for fast prototyping and testing

- •**Open source**: fluke is an open-source Python package;
- Easy to use: fluke is designed to be extremely easy to use out of the box;
- Easy to extend: fluke is designed to minimize the overhead of adding new algorithms;
- •**Up-to-date**: fluke comes with several (30+) state-of-the-art federated learning algorithms and datasets and it is regularly updated to include the latest affirmed techniques;
- Easy to read: the source code of the algorithms is written to mimic as close as possible the description in the reference papers.







fluke is on PyPi!

Install it using a single command



... or by cloning the repo







fluke CLI

You can run your experiment outright with a single command!



(*) If you cloned the repo, the command (launched from the fluke folder) is \$ python -m fluke.run -config exp.yaml federation algorithm.yaml

command

Configuration files

Two YAML files for everything you want to configure

logger setting



Default configuration files can be downloaded using the command: fluke-get





Configuration files

Two YAML files for everything you want to configure

exp.yaml	
<pre>data: dataset: name: mnist path: ./data distribution: name: iid</pre>	 dataset and data distribution configu
exp: device: cpu seed: 42	— general settings
eval: •	— evaluation settings
logger: name: Log	— logger setting
<pre>protocol: eligible_perc: 0.2 n_clients: 10 n_rounds: 10</pre>	 federated protocol configuration

uration client-side	
s hyper-parameters —	
algorithm name —	

Default configuration files can be downloaded using the command: fluke-get



fluke CLI – not only federation

You can run the "same" experiment without the federation for comparison



(*) The number of epochs can be set by the user via an option of the command, e.g., -epochs=100

same experiment but without the federation the number of epochs client-side are calculated* as n_rounds * eligible_perc * local_epochs

Example: FedAVG on MNIST

Fluke comes with many downloadable configuration files ready to be used/modified



(*) If you want to know all the available default configuration files use the command \$ fluke-get list

configuration file (named fedavg.yaml)

fluke logging

Performance can be logged on your preferred tool



communication cost*





(*) The communication cost is estimated as the number fo floating points numbers exchanged by the entire federation. (**) Currently, fluke supports only classification but it is straightforward to extend to other tasks. (***) System performance are automatically logged by W&B and ClearML.



fluke python API

The python API offers all you need to implement and test your FL ideas



https://github.com/makgyver/fluke



SCAN ME

30+



fluke server

Code readability is a key feature of fluke

Algorithm 1 FederatedAveraging. The K clients are indexed by k; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

Server executes:
initialize
$$w_0$$

for each round $t = 1, 2, ...$ do
 $m \leftarrow \max(C \cdot K, 1)$
 $S_t \leftarrow (\text{random set of } m \text{ clients})$
for each client $k \in S_t$ in parallel do
 $w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$
 $m_t \leftarrow \sum_{k \in S_t} n_k$
 $w_{t+1} \leftarrow \sum_{k \in S_t} \frac{n_k}{m_t} w_{t+1}^k$

McMahan et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS 2017. (*) This is a polish version of the fluke source code.





fluke client

Code readability is a key feature of fluke



McMahan et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS 2017. (*) This is a slightly polish version of the fluke source code.





fluke python API - Dataset loading & splitting



(*) fluke currently supports the following built-in datasets: MNIST, MNIST-M, SVHN, FEMNIST, EMNIST, CIFAR10, CIFAR100, Tiny Imagenet, Shakespeare, Fashion MNIST, and CINIC10.

fluke python API - Federated algorithm



fluke python API - Hyper-parameters

You can load the hyper-parameters from file or hard-coding them

(*) fluke can also handle cases where clients and server own different models (like sub-network of the overall model)

Hyper-parameters from file
I import yaml
With open("myconfig.yaml") as f:
Config_alg = yaml.safe_load(f)
Hyperparams = DDict(**config_alg)

client specific hyper-parameters, including the optimizer and the scheduler

server specific hyper-parameters

fluke python API - Logging

Logging is handled using callbacks (i.e., design pattern Observer)

this is the default logger (on console) but you can also log on **W&B**, **Tensorboard** or **ClearML**

the loggers in fluke only log evaluation results

and the communication channel

fluke python API - Start the training

fluke - Adding a new FL algorithm

You just need to implement the core part of your algorithm as described in the paper

•••	Define your client	
1 from fl 2 3 class M 4 5 def 6 7 8 9 10 11 12 13 14 def 15	<pre>.uke.client import Client AyClient(Client): *init(index: int,</pre>	1 from fluke.se 2 3 class Myserve 4 5 defini 6 7 8 9 10 11 12 13 def aggre 14
16 17 def 18 19 20 def 21 22	<pre>send_model(self) -> None: fit(self, override_local_epochs: int = 0) -> float: </pre>	

```
Define your algorithm
                                                        Define your server
                                                         1 class MyFLAlgo(CentralizedFL):
erver import Server
                                                         2
                                                               def get_server_class(self):
                                                         3
ver(Server):
                                                                   return MyServer
                                                         4
                                                         5
it__(self,
                                                               def get_client_class(self):
                                                         6
    model: torch.nn.Module,
                                                                   return MyClient
                                                         7
    test_set: FastDataLoader,
    clients: Iterable[Client],
    weighted: bool = False,
    **kwargs: dict[str, Any]):
egate(self, eligible: Iterable[Client]) -> None:
```

You just need to implement what characterise your FL algorithm

Kafè has been presented at ECML PKDD 2024!

that is already implemented in fluke.server.Server*

this is the standard behaviour of a

Require: T communication rounds, E local epochs, B local batchsize, h bandwith of KDE, m number of clients participating in aggregation. typical client selection process, 1: Server execute: Initialize model w^0 2: 3: for t = 1, ...T do $m \leftarrow max([C] \times K, 1)$ 4: 5: $S_m \leftarrow$ random selection of m clients Send $w^{(t-1)}$ to all clients. 6: 7:for chosen client $k \in S_m$ in parallel do $w_k^{f,(t)}, w_k^{c,(t)} \leftarrow \text{LocalUpdating}(w^{(t-1)})$ 8: this must be implemented !! 9: Model aggregation: 10: $w_g^{f,(t)} \leftarrow \sum_{k \in S_m} \frac{n_k}{n} w_k^{f,(t)}.$ 11: $w_g^{c,(t)} \leftarrow \mathbf{KAFE}(h, \frac{n_k}{n} w_k^{c,(t)})$ 12:Update $w_{g}^{(t)} = (w_{g}^{f,(t)}, w_{g}^{c,(t)})$ 13: end for 14:15:end for 16: FedAVG client, that is already -17: **LocalUpdating** $(w^{(t-1)})$: implemented in fluke.client.Client for e = 1, 2, ...E - 1 do 18:for each batch B do 19: $w_k^{(t)} \leftarrow w^{(t-1)} - \eta \nabla \ell(w^{(t-1)}, b).$ 20: 21: end for 22:end for **return** $w_k^{(t)} = (w_k^{f,(t)}, w_k^{c,(t)})$ 23: Pian Qi , et al. KAFÈ: Kernel Aggregation for FEderated. In ECML-PKDD 2024

Algorithm 1 KAFÈ

Kafè is a FL algorithm presented at ECML PKDD 2024!

def aggregate(self, eligible: Iterable[Client]) -> None: avg_model_sd = OrderedDict() clients_sd = self.get_client_models(eligible) weights = self._get_client_weights(eligible) # get last layer of m clients' weights last_layer_weight_name = list(clients_sd[0].keys())[-2] last_layer_bias_name = list(clients_sd[0].keys())[-1] for key in self.model.state_dict().keys(): if key in (last_layer_weight_name, last_layer_bias_name): continue for i, client_sd in enumerate(clients_sd): if key not in avg_model_sd: avg_model_sd[key] = weights[i] * client_sd[key] else: avg_model_sd[key] = avg_model_sd[key] + weights[i] * client_sd[key]

Kafè Server

Kafè is a FL algorithm presented at ECML PKDD 2024!

$$w_g^{c,(t)} \leftarrow \mathbf{KAF}\mathbf{\dot{E}}(h, \frac{n_k}{n} w_k^{c,(t)}).$$

Classification layers aggregation. The m classification layers of the m local models can be denoted as $\{w_1^{c,(t)}, w_2^{c,(t)}, ..., w_k^{c,(t)}, ...\}$. To evaluate the probability density function $\hat{f}(\cdot)$ for these classification layers w^c , we employ KDE as follows:

$$\hat{f}(w^{c}) = \frac{1}{mh^{d}} \sum_{k \in S_{m}^{(t)}} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(5)

where d denotes the dimension of the samples, similar to Eq. (1). In this context, d corresponds to the dimension of $w_k^{c,(t)}$ after flattening. To account for the varying contributions of the classification layers from different local models, we introduce weighting factors $\frac{n_k}{n}$ to the KDE formulation. Consequently, Eq. (5) is transformed into Eq. (6).

$$\hat{f}(w^{c}) = \frac{1}{h^{d}} \sum_{k \in S_{m}^{(t)}} \frac{n_{k}}{n} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(6)

Next, by sampling m new samples from the KDE and averaging them, we obtain the new classification layer $w_g^{c,(t)}$ for the global model. Lastly, the global

•••	Kafè Server
1 class KafeServer(Server):	
2 3 def 4 5 6 7 8 9 10 11	<pre>init(self,</pre>
31 32 33 34 35 36 37 38 39 40 41 42 43 40 41 42 43 44 45 46 47 48 49 50 51 52 53 51 52 53 54 55 56 57 58	<pre>w_last_layer = [] b_last_layer = [] for csd in clients_sd: w_last_layer.append(np.array(csd[last_layer_weight_name])) b_last_layer = np.array(w_last_layer).reshape(len(w_last_layer), -1) b_last_layer = np.array(b_last_layer).reshape(len(b_last_layer), -1) # using KDE get the kernel density of last layers kde_w = KernelDensity(kernel='gaussian',</pre>

Kafè is a FL algorithm presented at ECML PKDD 2024!

1 class KafeServe
2
3 definit_
4
5
6
7
8
9 super()
10
11 self.hy
- 10

 $w_g^{c,(t)} \leftarrow \mathbf{KAFE}(h, \frac{n_k}{n} w_k^{c,(t)}).$

```
Kafè Server
er(Server):
__(self,
  model: torch.nn.Module,
  test_set: FastDataLoader,
  clients: Iterable[Client],
  weighted: bool = False,
  bandwidth: float = 1.0):
).__init__(model=model, test_set=test_set,
          clients=clients, weighted=weighted)
yper_params.update(bandwidth=bandwidth)
```


Kafè is a FL algorithm presented at ECML PKDD 2024!

$$w_g^{c,(t)} \leftarrow \mathbf{KAF}\mathbf{\dot{E}}(h, \frac{n_k}{n} w_k^{c,(t)}).$$

Classification layers aggregation. The m classification layers of the m local models can be denoted as $\{w_1^{c,(t)}, w_2^{c,(t)}, ..., w_k^{c,(t)}, ...\}$. To evaluate the probability density function $\hat{f}(\cdot)$ for these classification layers w^c , we employ KDE as follows:

$$\hat{f}(w^{c}) = \frac{1}{mh^{d}} \sum_{k \in S_{m}^{(t)}} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(5)

where d denotes the dimension of the samples, similar to Eq. (1). In this context, d corresponds to the dimension of $w_k^{c,(t)}$ after flattening. To account for the varying contributions of the classification layers from different local models, we introduce weighting factors $\frac{n_k}{n}$ to the KDE formulation. Consequently, Eq. (5) is transformed into Eq. (6).

$$\hat{f}(w^{c}) = \frac{1}{h^{d}} \sum_{k \in S_{m}^{(t)}} \frac{n_{k}}{n} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(6)

Next, by sampling m new samples from the KDE and averaging them, we obtain the new classification layer $w_g^{c,(t)}$ for the global model. Lastly, the global

•••	Kafè Server
1 class KafeServer(Server):	
2 3 def 4 5 6 7 8 9 10 11	<pre>init(self,</pre>
31 32 33 34 35 36 37 38 39 40 41 42 43 40 41 42 43 44 45 46 47 48 49 50 51 52 53 51 52 53 54 55 56 57 58	<pre>w_last_layer = [] b_last_layer = [] for csd in clients_sd: w_last_layer.append(np.array(csd[last_layer_weight_name])) b_last_layer = np.array(w_last_layer).reshape(len(w_last_layer), -1) b_last_layer = np.array(b_last_layer).reshape(len(b_last_layer), -1) # using KDE get the kernel density of last layers kde_w = KernelDensity(kernel='gaussian',</pre>

Kafè is a FL algorithm presented at ECML PKDD 2024!

context, d corresponds to the dimension of $w_k^{c,(t)}$ after flattening. To account for the varying contributions of the classification layers from different local models, we introduce weighting factors $\frac{n_k}{n}$ to the KDE formulation. Consequently, Eq. (5) is transformed into Eq. (6).

Kafè is a FL algorithm presented at ECML PKDD 2024!

$$w_g^{c,(t)} \leftarrow \mathbf{KAF}\mathbf{\dot{E}}(h, \frac{n_k}{n} w_k^{c,(t)}).$$

Classification layers aggregation. The m classification layers of the m local models can be denoted as $\{w_1^{c,(t)}, w_2^{c,(t)}, ..., w_k^{c,(t)}, ...\}$. To evaluate the probability density function $\hat{f}(\cdot)$ for these classification layers w^c , we employ KDE as follows:

$$\hat{f}(w^{c}) = \frac{1}{mh^{d}} \sum_{k \in S_{m}^{(t)}} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(5)

where d denotes the dimension of the samples, similar to Eq. (1). In this context, d corresponds to the dimension of $w_k^{c,(t)}$ after flattening. To account for the varying contributions of the classification layers from different local models, we introduce weighting factors $\frac{n_k}{n}$ to the KDE formulation. Consequently, Eq. (5) is transformed into Eq. (6).

$$\hat{f}(w^{c}) = \frac{1}{h^{d}} \sum_{k \in S_{m}^{(t)}} \frac{n_{k}}{n} K\left(\frac{w_{k}^{c,(t)} - w^{c}}{h}\right)$$
(6)

Next, by sampling m new samples from the KDE and averaging them, we obtain the new classification layer $w_g^{c,(t)}$ for the global model. Lastly, the global

•••	Kafè Server
1 class KafeServer(Server):	
2 3 def 4 5 6 7 8 9 10 11	<pre>init(self,</pre>
31 32 33 34 35 36 37 38 39 40 41 42 43 40 41 42 43 44 45 46 47 48 49 50 51 52 53 51 52 53 54 55 56 57 58	<pre>w_last_layer = [] b_last_layer = [] for csd in clients_sd: w_last_layer.append(np.array(csd[last_layer_weight_name])) b_last_layer = np.array(w_last_layer).reshape(len(w_last_layer), -1) b_last_layer = np.array(b_last_layer).reshape(len(b_last_layer), -1) # using KDE get the kernel density of last layers kde_w = KernelDensity(kernel='gaussian',</pre>

Kafè is a FL algorithm presented at ECML PKDD 2024!


```
w_last_layer_new = np.mean(kde_w.sample(len(w_last_layer)), axis=0)
b_last_layer_new = np.mean(kde_b.sample(len(b_last_layer)), axis=0)
avg_model_sd[last_layer_weight_name] = torch.tensor(w_last_layer_new.reshape(
    clients_sd[0][last_layer_weight_name].shape))
avg_model_sd[last_layer_bias_name] = torch.tensor(b_last_layer_new.reshape(
    clients_sd[0][last_layer_bias_name].shape))
self.model.load_state_dict(avg_model_sd)
```

Testing Kafè in fluke

You just need to define the configuration files and use the fluke CLI

fluke results (W&B plot)

Running Kafè

1 \$ fluke --config exp.yaml federation kafe.yaml

Give it a try, you won't regret it!

fluke 0.3.0 is now available!

30+ FL algorithms

> propose your FL algorithm to be included in fluke!

11 datasets

https://github.com/makgyver/fluke https://makgyver.github.io/fluke/

All the icons have been downloaded from www.flaticon.com

[quick] Icon made by Cuputo from www.flaticon.com [chart] Icon made by Freepik from www.flaticon.com [idea] Icon made by Freepik from www.flaticon.com [network cost] lcon made by juicy_fish from www.flaticon.com [performance] lcon made by juicy_fish from www.flaticon.com [programming] lcon made by juicy_fish from www.flaticon.com [close] Icon made by Pixel Perfect from www.flaticon.com [check-mark] lcon made by lan June from www.flaticon.com [pause] lcon made by bqlqn from www.flaticon.com [jigsaw] Icon made by monkik from www.flaticon.com